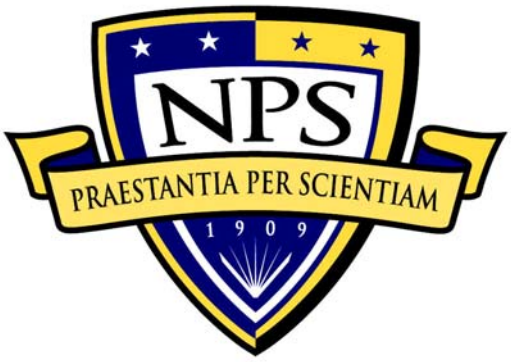
2010-09

Striking the right balance : fusion centers and privacy

Skahill, Tina M.

Monterey, California. Naval Postgraduate School



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

STRIKING THE RIGHT BALANCE: FUSION CENTERS AND PRIVACY

by

Tina M. Skahill

September 2010

Thesis Advisor: John Rollins
Second Reader: Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Striking the Right Balance: Fusion Centers and Privacy		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Tina M. Skahill			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

After the events of 9/11, the number of fusion centers rapidly multiplied. As a result, state and local agencies that operated the centers adopted a myriad of policies. This thesis seeks to answer how fusion centers can implement policies as to operational structure and transparency that simultaneously safeguard against abuse of citizens' privacy while facilitating the collection, maintenance, and dissemination of information.

Two methods of research are utilized: policy analysis and policy options analysis. This thesis examines existing federal guidelines, federal case law, and various federal statutes and regulations. Moreover, the thesis explores three policy options as possible decision-making tools for fusion centers: 1) mandatory federal guidelines, 2) imposition of a balancing test and administrative review process, and 3) a compulsory reasonable-suspicion requirement. In the end, this thesis recommends imposition of all three policies.

14. SUBJECT TERMS Fusion Center Privacy Policies, Mandatory Guidelines, Balancing Test, Administrative Review, Reasonable Suspicion			**15. NUMBER OF PAGES** 113
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approve for public release; distribution is unlimited

STRIKING THE RIGHT BALANCE: FUSION CENTERS AND PRIVACY

Tina M. Skahill
Chief of CAPS Project Office, Chicago Police Department, Chicago, Illinois
B.S., Loyola University of Chicago, 1982
J.D., DePaul University College of Law, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Tina M. Skahill

Approved by: John Rollins
Thesis Advisor

Lauren Wollman
Second Reader

Harold A. Trinkunas, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

After the events of 9/11, the number of fusion centers rapidly multiplied. As a result, state and local agencies that operated the centers adopted a myriad of policies. This thesis seeks to answer how fusion centers can implement policies as to operational structure and transparency that simultaneously safeguard against abuse of citizens' privacy while facilitating the collection, maintenance, and dissemination of information.

Two methods of research are utilized: policy analysis and policy options analysis. This thesis examines existing federal guidelines, federal case law, and various federal statutes and regulations. Moreover, the thesis explores three policy options as possible decision-making tools for fusion centers: 1) mandatory federal guidelines, 2) imposition of a balancing test and administrative review process, and 3) a compulsory reasonable-suspicion requirement. In the end, this thesis recommends imposition of all three policies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....2
1. Complex Governance Structures and Transparency....2
2. Lack of Consistency and Coherence in Government Guidelines....3
B. RESEARCH QUESTION....4
C. PRACTICAL SIGNIFICANCE OF THE RESEARCH....4
D. METHODOLOGY....5
1. Policy Analysis....5
2. Policy Options Analysis....6
a. Mandatory Guidelines....6
b. Balancing Test and Administrative Review....6
c. Reasonable Suspicion Requirement....7
d. Analysis Criteria....7
E. LITERATURE REVIEW....7
1. Risk and Activities....8
2. Principles....8
3. Gaps in Literature....9
a. Community Policing and Fusion Centers....9
b. Agency-Initiated Privacy Impact Assessments....11

II. THE STATUS QUO....13
A. THE FUNDAMENTALS OF PRIVACY....13
1. Evolution of Fusion Centers....13
a. The General Mission of Fusion Centers....13
b. Undertaking Domestic Intelligence Activities....15
2. Privacy Concerns and Considerations....18
a. Case Law....18
b. Federal Statutes....21
B. CASE STUDIES....23
1. Chicago Fusion Center Privacy Policy....24
2. California's Fusion Center Privacy Policy....24
3. Miami-Dade Fusion Center Privacy Policy....25
4. Comprehensive Policy Model....25
C. GOVERNANCE STRUCTURE AND TRANSPARENCY ISSUES....26
1. American Civil Liberties Union Concerns....26
2. Electronic Privacy Information Center Concerns....29
3. Addressing ACLU and EPIC Concerns....30

III. PROPOSED OPTIONS....31
A. ESTABLISHING MANDATORY DEPARTMENT OF JUSTICE AND DEPARTMENT OF HOMELAND SECURITY PRIVACY GUIDELINES....31
1. Best Practices Utilizing DHS and DOJ Guidelines....31

2. Federal Regulation Pros and Cons 32
B. UTILIZING A BALANCING TEST AND ADMINISTRATIVE REVIEW PROCESS 32
1. Elements of the Balancing Test 33
2. Administrative Review Process 33
3. Pros and Cons of Balancing Test and Administrative Review 34
C. IMPOSING A REASONABLE-SUSPICION REQUIREMENT 34
1. Definition of Reasonable Suspicion Under Criminal Law 34
2. Application of Reasonable Suspicion Requirement to Fusion Centers 35
3. Pros and Cons of a Reasonable Suspicion Requirement 35
IV. CHOOSING THE RIGHT POLICY 37
A. MANDATORY DOJ AND DHS GUIDELINES OPTION 38
B. BALANCING TEST AND ADMINISTRATIVE REVIEW OPTION 38
C. REASONABLE-SUSPICION OPTION 39
V. THE RECOMMENDED POLICY 41
A. MANDATORY FUSION CENTER GUIDELINES 41
B. MANDATORY BALANCING TEST AND ADMINISTRATIVE REVIEW POLICY 41
C. MANDATORY REASONABLE SUSPICION REQUIREMENT 42
D. CONCLUSION 42
APPENDIX A. CHICAGO POLICE DEPARTMENT'S CRIME PREVENTION AND INFORMATION CENTER PRIVACY POLICY 45
APPENDIX B. CALIFORNIA'S FUSION CENTER PRIVACY POLICY 53
APPENDIX C. MIAMI-DADE POLICE DEPARTMENT'S FUSION CENTER PRIVACY POLICY 85
LIST OF REFERENCES 93
INITIAL DISTRIBUTION LIST 97

LIST OF TABLES

Table 1. Privacy Policies Comparison 24
Table 2. Comparison Matrix of Proposed Options 37

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
CFR	Code of Federal Regulations
CPD	Chicago Police Department
CPIC	Crime Prevention and Information Center
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
EPIC	Electronic Privacy Information Center
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FBI	Federal Bureau of Investigation
GAO	General Accountability Office
ISE	Information Sharing Environment
LAPD	Los Angeles Police Department
MDPD	Miami-Dade Police Department
MOU	Memorandum of Understanding
NCISP	National Criminal Intelligence Sharing Plan
NDA	Non-Disclosure Agreement
PIA	Privacy Impact Assessment
SAR	Suspicious Activity Report
STTAS	State Terrorism Threat Assessment System

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to thank the instructors and staff of the Center of Homeland Defense and Security for their invaluable assistance and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The 9/11 Commission identified four types of failure that contributed to the successful attacks on the World Trade Center and the Pentagon: failures in imagination, policy, capabilities, and management (National Commission on Terrorist Attacks upon the United States [9/11 Commission], 2004). The Commission also made a number of recommendations designed to prevent such failures in the future. The creation and operation of fusion centers was a concept not included in the recommendations. Nevertheless, the Commission did acknowledge the critical nature of intelligence analysis and the need for information sharing. The Commission report stated: "The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots——is the human or systemic resistance to sharing information" (9/11 Commission, 2004, p. 416).

According to the Department of Homeland Security (DHS) as of 2008, there were 72 fusion centers throughout the United States. DHS defines a fusion center as "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity" (United States Department of Homeland Security [USDHS], 2008, p. 4). Fusion centers are not operated by the federal government, though federal agencies such as the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) often participate. Furthermore, many fusion centers rely entirely upon federal grants to support operations. State or local law enforcement agencies often direct the operation of the centers, and fusion centers vary in structure and operational procedures (and policies) from state to state. Nevertheless, fusion centers do share one aspect in common—the collection, analysis, and dissemination of information derived from a variety of sources. These activities have a profound impact upon the Fourth Amendment right to privacy guaranteed by the U.S. Constitution and the application of this right to the states via the Fourteenth Amendment.

The 9/11 Commission recognized the need to protect citizens' privacy while sharing information. In the 9/11 Commission Report (2004), the commission recommended that "as the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared" (9/11 Commission, 2004, p. 394). This thesis focuses upon the development and implementation of the privacy policies of fusion centers and the need to simultaneously balance the protection of privacy and the factiliation of information sharing.

A. PROBLEM STATEMENT

1. Complex Governance Structures and Transparency

The most controversial privacy issues regarding fusion centers derive from the complex governance structures and the transparency of the centers' activities, i.e., the collection, analysis, and dissemination of information (Andino, 2008). For example, in 2008 the Electronic Privacy Information Center (EPIC) filed a Freedom of Information Act (FOIA) lawsuit against the Virginia State Police for refusing to provide requested information concerning the agency's interaction with the Department of Homeland Security (DHS) and the Department of Justice (DOJ) as to the fusion center's operation (Andino, 2008). Through the lawsuit the organization obtained a copy of a memorandum of understanding between the FBI and the Virginia State fusion center that required the center to consult with the FBI before responding to a FOIA request (Electronic Privacy Information Center [EPIC], 2009). By agreeing to the memorandum, the Virginia State fusion center significantly reduced the level of transparency as to its activities. This transparency was needed to ensure that the center provided adequate protection of privacy rights.

Some fusion centers include private agencies as participants. Such an arrangement results in a complex governance structure because private agencies operate under a different governance structure than public agencies. These structures may compete with one another on several issues, such as data security. According to an American Civil

Liberties Union report entitled "What's Wrong with Fusion Centers?" some centers utilize private companies to store and analyze data that includes personal information such as birth dates, social security numbers, credit reports, and employment history. For example, the Texas Department of Homeland Security contracted with Northrop Grumman Corporation for such purposes after a number of evacuees from Hurricane Katrina arrived in Texas (German & Stanley, 2007). According to the *Texas Observer*, the project was unsuccessful due to security concerns surrounding the data: it was unclear who at the corporation had access to the data or the present status of the data (German & Stanley, 2007).

2. Lack of Consistency and Coherence in Government Guidelines

The federal government has recommended a number of privacy guidelines to address the crucial issues of governance structures and transparency via DHS and DOJ. There is no shortage of federal guidelines on the subject of privacy. DHS and DOJ's Fusion Center Guidelines (USDHS & DOJ, 2006), DOJ's Privacy and Civil Liberties Policy Development Guide and Implementation Template (DOJ, 2008), and DHS's Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative (USDHS, 2008) provide a few examples. However, there is an overall lack of consistency and coherence as to the application of these guidelines. DHS has attempted to address the inconsistency. "DHS provides staffing, technical, and privacy and civil liberties training to fusion centers and collaborates with the Global Justice Information Sharing Initiative ("Global"), a DOJ entity, to deliver training" (Andino, 2008, p. 2). However, individual agencies that participate in fusion centers often adhere to their individual state's privacy laws and agency's policies. Such adherence encourages "policy shopping" according to the ACLU (German & Stanley, 2007). Agencies may not host the data, as it would be prohibited by their individual agency's policy, but access the data through other participants. For example, according to a *Washington Post* article "Centers Tap into Personal Databases," the Ohio fusion center has been granted access to an FBI "secret level repository" (O'Harrow, 2008). Under

their agency's policy, the Ohio State Police is not privy to such information. However, through their partnership with the FBI, the agency has access to the information contained in this repository.

Such arrangements contribute significantly to the inconsistency and incoherence of guidelines. Permitting a fusion center to circumvent state law or operate outside of its established, approved policies contributes to the erosion of the very principles that state law or agency policy seek to uphold. Moreover, public discourse is stifled as to the appropriateness of such access because the official, transparent channels are avoided.

B. RESEARCH QUESTION

How can fusion centers implement policies as to operational structure and transparency that simultaneously guard against the abuse of privacy rights and facilitate the collection, analysis, and dissemination of information?

C. PRACTICAL SIGNIFICANCE OF THE RESEARCH

This thesis will offer an in-depth analysis of the existing policies concerning privacy at fusion centers and the recommended guidelines by DOJ and DHS. It will also examine possible strategies and policies to address consistency and coherence problems surrounding governance structures and transparency issues of fusion centers' collection, maintenance, and dissemination of personal data. In addition, the thesis will recommend the imposition of a policy designed to strike a balance between citizens' privacy rights and the homeland security objectives of fusion centers. Directors of fusion centers will find this thesis useful in designing policies and procedures to address privacy concerns. Moreover, the thesis will contribute to the body of literature addressing fusion centers by providing a comparative analysis of fusion center policies and recommended DHS and DOJ guidelines.

D. METHODOLOGY

1. Policy Analysis

In order to properly assess the privacy guidelines and possible alternatives, it is best to begin with a comprehensive review of those guidelines currently in place in order to identify the strengths and weaknesses of those policies and to evaluate possible solutions that emphasize the strengths and eradicate the weaknesses. The research method best suited for such an endeavor is a policy analysis. By thoroughly examining the privacy policies of major fusion centers that participated in the Suspicious Activity Report Support and Implementation Project (Chicago, Los Angeles, and Miami-Dade), it will be possible to understand the strengths and weaknesses of these existing policies.[1] The Suspicious Activity Report (SAR) Support and Implementation Project's aim was to develop a uniform approach to the reporting of suspicious activity (SAR Support and Implementation Project [SAR], 2008). The aim of this thesis is similar in that it seeks to address a uniform method for fusion centers to protect privacy rights while facilitating the collection, analysis, and dissemination of information. For this reason, the privacy policies of those fusion centers involved in the project were selected for analysis. Furthermore, a more in-depth appraisal of this subject is afforded through a review of the aforementioned fusion centers' privacy policies as to collection, retention, and dissemination of personal data, an examination of local, state, and federal legal requirements concerning privacy, and an assessment of the degree of transparency and openness of those policies and procedures to the public.

In addition, an extensive evaluation of DOJ- and DHS-recommended privacy guidelines is required, as delineated in the Department of Homeland Security and Department of Justice's Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era (USDHS & DOJ, 2006), the Privacy and Civil Liberties Policy Development Guide and Implementation Template (DOJ, 2008), and the Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional

[1] The Boston Regional Information Center is in the process of reviewing its privacy policy; therefore, the policy is unavailable at this time.

Fusion Center Initiative (USDHS, 2008) . An analysis of these recommended guidelines, compared to policies actually implemented in the fusion centers, enables one to gauge the effectiveness of implementing a standard guideline across the nation.

2. Policy Options Analysis

a. Mandatory Guidelines

The privacy guidelines recommended by the Department of Justice and the Department of Homeland Security are not mandatory. As a result, fusion centers utilize a variety of privacy guidelines. In order to ensure some consistency in the application of these guidelines, DHS offers training and technical assistance for fusion center participants. "Global [U.S. Department of Justice's Global Justice Information Sharing Initiative] resources support development of common standards and protocols for collecting, analyzing, and sharing information (and associated training) and the creation of intelligence products for customers" (DOJ, 2009, p. 11). In order to further support such standardization, one solution proposes to require mandatory imposition of the DOJ and DHS guidelines.

b. Balancing Test and Administrative Review

Another possible solution is a fusion center policy requiring the imposition of a balancing test coupled with an administrative review process prior to the collection and maintenance of personal information. The balancing test would be utilized in conjunction with the DHS and DOJ guidelines in order to ascertain, given a particular set of circumstances, to what extent privacy rights should be compromised. In other words, does the need to prevent terrorism, crime, or other hazards by collecting, maintaining, or disseminating particular information outweigh the public's right to privacy?

c. Reasonable Suspicion Requirement

Under the final proposed policy, collection, retention, and dissemination of information by all fusion centers would only be permitted if reasonable suspicion exists that the individual has committed, is committing, or is about to commit a criminal act. This is the current policy of Chicago's fusion center. By imposing this recognizable standard upon all fusion centers, uniform application of DOJ- and DHS-recommended privacy guidelines may emerge.

d. Analysis Criteria

In deciding which policy to recommend, it is best to judge the proposed courses of action by their impact upon the following areas: consistency and coherence of governance structures and transparency. Both variables are equally important to the protection of the public's right to privacy. The recommended policy must be simple to apply and provide a consistent method for the protection of privacy rights. Furthermore, the recommended policy must afford a coherent view of the fusion center's governance structures in order to ensure that, should fusion centers fail to adhere to privacy policies, the public is alerted as to what corrective action it should take.

E. LITERATURE REVIEW

Although fusion centers differ as to whether they adopt an all-hazards, crime-oriented, or anti-terrorism focus, the centers display similarities as to the functions performed at these facilities. The publications acknowledge that the collection of intelligence and the use of private-sector data cause concern about privacy rights. Because of these concerns, many government publications delineate guidelines for the collection of intelligence and the use of data in order to achieve the fusion center's goals while simultaneously protecting citizens' right to privacy. Nongovernmental publications tend to point out the deficiencies in the existing systems as opposed to proposing specific

guidelines. In reviewing the literature, the publications discuss two primary areas of the intelligence process: risks and activities associated with the intelligence process and core principles of privacy.

1. Risk and Activities

The Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment identifies six activities relating to information sharing (collection, retention, production, usage, sharing, and management) that impact privacy (Information Sharing Environment [ISE], 2008). Federal agencies in the intelligence community regularly conduct these activities, and state and regional fusion centers participate in such activities as well.

Most of the publications tend to identify specific risks to privacy. For example, the Department of Homeland Security's Privacy Impact Assessment identifies seven such risks: justification for fusion centers, ambiguous lines of authority, participation of the military and private sector, data mining, excessive secrecy, inaccurate or incomplete information, and mission creep (USDHS, 2008). Even nongovernmental agencies identify these same risks. In "What's Wrong with Fusion Centers?" the American Civil Liberties Union (ACLU) discussed each of the risks identified by DHS's Privacy Impact Assessment (German & Stanley, 2007). Where publications tend to differ is in their proposed solutions to mitigating these risks.

2. Principles

Some documents address core principles for federal agencies in the intelligence community. Though these documents do not apply per se to state and regional fusion centers, the core principles may be applied to such systems. For example, the Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment points out that "in order to share information in the ISE, nonfederal entities – including state, local, tribal, and foreign governments—develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the ISE Privacy Guidelines" (ISE, 2008, p.2). In order to be effective, fusion centers

must be able to share information within the information-sharing environment, with the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), and Federal Emergency Management Agency (FEMA), for example.

Specific privacy principles applicable to fusion centers can be found in guideline 8 in the Department of Homeland Security and Department of Justice's Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era . According to the guideline, fusion centers should "develop, publish, and adhere to a privacy and civil liberties policy" (USDHS & DOJ, 2006, p. 41). Guideline 8 espouses eight core principles regarding privacy and civil liberties: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. These principles tie directly to the activities of a fusion center, i.e., those delineated in the ISE Privacy Guidelines.

Underlying core privacy principles are also identified by nongovernmental organizations, such as the Electronic Privacy Information Center (EPIC), for example. In 2007, Lillie Coney delivered a statement on behalf of the organization to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. According to Coney (2007), the Privacy Act of 1974, Public Law 93-579, identifies four procedural and substantive rights applicable to computerized databases in use by fusion centers: 1) requiring agencies to reveal information concerning an individual upon his request, 2) compelling agencies to adhere to fair information practices, 3) placing restrictions upon agencies as to information sharing, and 4) granting citizens the right to sue agencies for violations.

3. Gaps in Literature

a. Community Policing and Fusion Centers

Fusion centers operate on a theory of expansive collaboration. The entities that participate in fusion centers vary, but most can be categorized as governmental or private sector. Among the governmental agencies, law enforcement (local or state) tends to lead the centers. Over the years, law enforcement has engaged in community policing

as a proactive strategy to address crime and disorder. The cornerstone of this strategy requires the consistent sharing of information and discussions with the community as to problems and solutions to address crime and disorder problems. Local law enforcement's participation in fusion centers presents these agencies with a dilemma. Federal partners, such as the FBI and DEA, have not been engaged with the public to the same degree as local law enforcement. The openness and sharing of information with the public that is essential to effective community policing efforts is stymied when it comes to fusion center activities. In large part, this is due to the other participants who are apprehensive about such openness. The use of memorandums of understanding (MOUs) between federal agencies and local law enforcement has been identified by some of the literature as a collaborative tool. But, according to some such as EPIC, these agreements permit local agencies to circumvent state law as to freedom-of-information requests.

Upon review of the guidelines issued by federal agencies such as DHS and DOJ, these documents fail to address the reconciliation of community-policing principles with fusion center operations. Rollins's Congressional Research Service Report recommends public outreach (Rollins, 2008). However, community policing involves more than public outreach. It permits citizens to actively identify and prioritize items of concern to be addressed by the community and law enforcement. This level of involvement does not appear to be present in fusion center operations, nor is it addressed in a review of the various government publications.

Another area of contention that appears to be ignored by the guidelines is the customers of the fusion centers. Repeatedly, the various guidelines identify customers as the participant agencies of the fusion centers. Law enforcement, however, has defined its customers as the public it serves. The guidelines are virtually silent as to these competing definitions. The public is concerned with transparency. The participating agencies are concerned with security. Transparency of fusion center operations and public involvement directly affects an agency's ability to gather information. The failure of guidelines to adequately address the competing principles of security and transparency results in inconsistencies among fusion centers.

b. Agency-Initiated Privacy Impact Assessments

There exists no shortage of federal guidelines on the subject of privacy. DHS and DOJ's Fusion Center Guidelines (2006), DOJ's Privacy and Civil Liberties Policy Development Guide and Implementation Template (2008), and DHS's Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative (2008) serve as examples. The guidelines call upon the fusion centers to conduct their own privacy impact assessment (PIA). In April of 2009, Director Robert Riegle of DHS's Office of Intelligence and Analysis testified before a committee examining the future of fusion centers, stating: "The DHS Privacy Office recommends that each fusion center conduct a PIA evaluating its own operations, make it available to the public, and then engage with its local communities." (Riegle, 2009). Neither Riegle, nor the guidelines recommending such self-conducted privacy-impact assessments, address the inherent problem with an agency conducting its own assessments, i.e., lack of impartiality. Furthermore, each state and local agency is responsible for ensuring adherence to its own laws and policies, including those affecting privacy. A citizen's right of redress is then mostly dependent upon individual fusion-center policies and state and local laws.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE STATUS QUO

A. THE FUNDAMENTALS OF PRIVACY

1. Evolution of Fusion Centers

Although state and local law enforcement agencies collected and analyzed information before September 11, 2001, the events of that day spurred these agencies to establish a more formal network to perform these tasks (Rollins, 2008). After 9/11, there were approximately 40 fusion centers (Rollins, 2008). Presently there exist 72 fusion centers. Primarily, state and local law enforcement agencies operate fusion centers. Federal agencies, such as the Federal Bureau of Investigation and DHS participate in the centers, but are not responsible for the centers' operations.

As an example, the Chicago Police Department operates a fusion center called the Crime Prevention and Information Center (CPIC). The Chicago Police Department identifies the FBI, DHS, Department of Defense, Immigration Customs Enforcement, Illinois State Police, Cook County Sheriff's Police, and the United States Coast Guard as dedicated partners. Federal transportation agencies and private security firms are identified as provisional partners (Chicago Police Department, 2007). Dedicated partners maintain a continuous presence at the CPIC. Provisional partners are utilized on a case-by-case basis, in particular during an emergency management incident.

Federal agencies may be partners in fusion centers with state, local, and tribal agencies, but the primary role of the federal government is to provide financial assistance through the grant system (Rollins, 2008). In addition, the federal government provides guidance and training to these entities.

a. The General Mission of Fusion Centers

Fusion centers primarily collect, analyze, and disseminate information. Some fusion centers concentrate on criminal and terrorist incidents. Others operate on an all-hazards basis. In 2006, the U.S. Department of Homeland Security and the U.S.

Department of Justice published Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era. The document identifies 18 guidelines for fusion centers:

1. Adhere to the National Criminal Intelligence Sharing Plan (NCISP) and other sector-specific information sharing guidelines, and perform all steps of the intelligence and fusion process.

2. Develop and embrace a mission statement and identify goals for the fusion center.

3. Create a representative governance structure that includes law enforcement, public safety, and the private sector.

4. Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety, and the private sector.

5. Utilize memorandums of understanding (MOUs), non-disclosure agreements (NDAs), or other types of agency agreements, as appropriate.

6. Leverage the databases, systems, and networks available via participating entities to maximize information sharing.

7. Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems.

8. Develop, publish, and adhere to a privacy and civil liberties policy.

9. Ensure the appropriate security measures are in place for the facility, data, and personnel.

10. Integrate technology, systems, and people.

11. Achieve a diversified representation of personnel based on the needs and functions of the center.

12. Ensure personnel are properly trained.

13. Provide a multitiered awareness and educational program to implement intelligence-led policing and developing and sharing information.

14. Offer a variety of intelligence services and products to customers.

15. Develop, publish, and adhere to a policies and procedures manual.

16. Define expectations, measure performance, and determine effectiveness.

17. Establish and maintain the center based on funding availability and sustainability.

18. Develop and implement a communication plan within the fusion center; among all involved law enforcement, public safety, and private sector agencies and entities; and with the general public. (USDHS & DOJ, 2006, pp. 5–7)

b. Undertaking Domestic Intelligence Activities

This thesis focuses on the 8h guideline: the development and implementation of a privacy policy. DHS and DOJ recommend adherence to the fair information practices delineated in the Privacy Policy Development Guide and the Privacy and Civil Rights Policy Template for Justice Information Systems as a means to safeguard privacy (USDHS & DOJ, 2006). These documents were developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative. According to the Global Initiative (2006), the fair information practices comprise the following eight principles: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) openness; (7) individual participation; and (8)

accountability. Adherence to the aforementioned principles, according to DHS and DOJ (2006), ensures baseline privacy protection. However, an examination of these principles illustrates their lack of specificity.

The Department of Homeland Security and DOJ (2006) recommend that the collection of personal data be limited to legal and fair methods. Also, if appropriate, fusion centers should collect the data with the subject's knowledge or approval. The collection limitation principle fails to delineate the criteria for determining legal and fair means of data collection.

The second principle addresses data quality. DHS and DOJ insist that the collected data be relevant to its proposed purpose and be accurate and complete. The data quality principle as explained in Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era fails to specify legitimate (or illegitimate) purposes for data collection (USDHS & DOJ, 2006). Neither does the document offer a method for determining legitimacy.

Likewise, the purpose specification principle also fails to specify legitimate purposes for data collection. It does, however, recommend that such purposes be determined at the time the data is collected (USDHS & DOJ, 2006).

The fourth principle of fair information practices restricts usage or dissemination of the information in accordance with the fusion center's governance structure, the subject's consent, or by authority of law (USDHS & DOJ, 2006). Nevertheless, DHS and DOJ offer no further explanation.

Similarly, the fifth principle recommends that personal information be protected by "reasonable" safeguards. However, it fails to explain how to determine that a safeguard is reasonable (USDHS & DOJ, 2006).

As to transparency DHS and DOJ state, "There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal

data, and the main purposes of their use, as well as the identity and usual residence of the data controller" (USDHS & DOJ, 2006, p. 41). DHS and DOJ fail to recommend how fusion centers should develop such practices and policies.

The seventh principle recommended in Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era is individual participation. This principle encompasses a great degree of specificity. DHS and DOJ contend that an individual has the right to ascertain from the fusion center whether the center maintains data relating to the individual. Furthermore, DHS and DOJ recommend that the fusion center provide the individual with the requested data "within a reasonable time, cost, and manner" (USDHS & DOJ, 2006, p. 41). Moreover, the agencies state that if a request for information is denied, a mechanism must be in place to challenge such a denial. In addition, if the individual successfully challenges the content of the data, the information should be deleted, corrected, or completed (USDHS & DOJ, 2006).

The final principle espoused by DHS and DOJ as to guideline 8 is accountability. Here, DHS and DOJ defer to the National Criminal Intelligence Sharing Plan (NCISP):

- Eliminate unnecessary discretion in decision making, guide the necessary discretion, and continually audit the process to ensure conformance with the policy.
- Ensure legitimacy—when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented.
- Clearly define the parameters of the policy.
- Acknowledge and address important issues that currently are not included in some existing criminal intelligence policies.

- Identify the decision points within the intelligence process and provide appropriate guidance and structure for each. (USDHS & DOJ, 2006)

As with the previous principles, the recommended steps regarding accountability fail to offer any specificity. No suggestions or recommendations exist as to how a fusion center should go about performing the delineated general tasks.

In 2008, the United States Information Sharing Environment (ISE) published the Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment. This guide offers specificity; however, the document is directed toward federal agencies. It addresses issues likely to arise at the federal level, but not the state, local, or tribal level. According to this document there exist the two stages of implementation: identification and demonstration of the privacy policy's framework and application of the privacy policy's framework (ISE, 2008).

2. Privacy Concerns and Considerations

An examination of federal court cases and statutes establishes the fundamental principles of the citizen's right to privacy. Adherence to these principles is required in the adoption of any recommended fusion-center policies. These policies are designed to balance privacy rights while simultaneously permitting fusion centers to effectively collect, analyze, and disseminate information. The cases and statutes below address the principle of "reasonableness" and its application to privacy rights.

a. Case Law

The Fourth Amendment of the United States Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized" (United States Constitution, art. 4). Over the years, the United States Supreme Court has addressed an individual's right to privacy under the Fourth Amendment.

Several landmark court cases address privacy. *Griswold v. Connecticut* (1965) is thought to be the case in which the U.S. Supreme Court established the right to privacy (Lane, 2009).Connecticut law made it a crime to dispense contraceptive information, even to married persons. The court held the law unconstitutional. Justice Douglas stated in the court's opinion: "We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system" (*Griswold v. Connecticut*, 381 U.S. 479, 486 (1965)).

In *Katz v. United States* (1967), Katz appealed his conviction of interstate gambling based upon information that the FBI had obtained from warrantless electronic surveillance of his telephone conversation inside a public phone booth. Katz asserted that the FBI violated the Fourth Amendment of the United States Constitution. The Supreme court agreed. "Writing for the court's majority, associate justice Porter Stewart identified a zone of privacy that surrounds each individual: 'Wherever a man may be,' he said, 'he is entitled to know that he will remain free from unreasonable searches and seizure' " (Lane, 2009, p. xiv). Katz had a reasonable expectation of privacy as to his conversation inside the phone booth even though the booth was visible to the public.

In *United States v. United States District Court* (1972), the Attorney General of the United States approved electronic, domestic surveillance on the ground of national security. The government claimed that this approval was sufficient and no warrant was required. The court disagreed and stated:

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner

> compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure. (*United States v. United States District Court,* 407 U.S. 297, 320, (1972)).

In *U.S. v. Miller,* 425 U.S. 435 (1976), the U.S. Supreme Court found that no reasonable expectation of privacy existed as to bank records, thereby permitting the records to be obtained via subpoena. Likewise, in 1979, the court held in *Smith v. Maryland,* 442 U.S. 735, that no warrant was needed to obtain telephone numbers, via pen register, called by a subject. No reasonable expectation of privacy existed for these numbers as the numbers were included in the subject's telephone bill.

In *Whelan v. Roe,* the U.S. Supreme Court upheld the 1972 New York State Controlled Substances Act, which required the state to collect names and addresses of persons who obtained controlled substances via a physician's prescription. This information was maintained in a computer file. The court rejected the claim that collection and maintenance of this information constituted an invasion of a patient's privacy (*Whelan v. Roe,* 429 U.S. 589 (1977)).

In 1989, the U.S. Supreme Court addressed whether FBI criminal identification records ("rap sheets") constituted personal information that could be exempted from disclosure to a third party under the Freedom of Information Act. The court stated: "The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded" (*U.S. Department of Justice v. Reporters Committee,* 489 U.S. 749, 771 (1989)).

Most recently, the U.S. Supreme Court decided *City of Ontario v. Quon* 560 U.S. ___ (2010). In this case, the police officer Quon asserted that he had a reasonable expectation of privacy to his text messages transmitted over his employer's (Ontario, California Police Department) communication device. Furthermore, he contended that his employer's seizure of these communications without a warrant violated the Fourth Amendment.

The court agreed that Quon had a reasonable expectation of privacy. It relied on *Skinner v. Railway Labor Executives' Ass'n,* 489 U.S. 602, 613–614 (1989) in stating that "the Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the government, without regard to whether the government actor is investigating crime or performing another function." Nevertheless, the court held that the Ontario Police Department's retrieval of the text messages without a warrant constituted a reasonable search and seizure.

In summary, the U.S. Supreme Court has established in a number of cases throughout the years that individuals have a right to privacy pursuant to the Fourth Amendment. Furthermore, when people have a reasonable expectation of privacy, government must have a warrant or exceptional reasons for invading the person's privacy. However, where no reasonable expectation of privacy exists, the government need not obtain a warrant.

b. Federal Statutes

The Privacy Act of 1974 (5 USC § 552a) applies only to federal agencies, but it serves as a foundation from which other statutes arose. The Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of personal information by federal agencies. Absent statutory exemptions, the act prohibits dissemination of information without the subject's consent. Some exemptions include information collected and disseminated for statistical purposes, criminal investigations, and routine use. In reality, "the Privacy Act requires each agency in possession of systems of records to publish for each system the routine uses to which the information might be put. Such notices are published in the *Federal Register*. Most citizens are unaware of these notices and their implications, with the result that they have little understanding of how information supplied by or about them to the government agencies might be used" (Relyea, 2002, p. 9). Nevertheless, individuals may review, request copies, or request correction of their records under the Privacy Act.

In 2008, the General Accounting Office (GAO) submitted a report identifying three key problems with the Privacy Act: 1) narrowly defined key terms, 2)

no assurance that usage of personal information is restricted to clearly defined purposes, and 3) no effective means of communication to the public. The office did, however, recommend several actions be taken to correct these problems:

- Revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- Setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- Establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices. (GAO, 2008)

Section 208 of the E-Government Act of 2002 (44 U.S.C. § 208) requires federal agencies to conduct privacy impact assessments when utilizing new or substantially altered systems handling personal information (Privacy Office, 2007). “A PIA should accomplish two goals: (1) it should determine the risks and effects of collecting, maintaining, and disseminating personally identifiable information via an electronic system; and (2) it should evaluate protections and alternative processes for handling information to mitigate potential privacy risks” (Privacy Office, 2007, p. 7).

Although the Privacy Act of 1974 and the E-Government Act of 2002 apply to federal agencies, neither applies to state and local agencies managing fusion centers. However, the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) apply to federal agencies and nonfederal agencies who receive federal funds for their intelligence systems. Fusion centers receive federal monies in order to operate their intelligence systems. Title 28 of the Code of Federal Regulations states: “A project shall collect and maintain criminal intelligence information concerning an individual only if

there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity" (28 CFR § 23.20 (a)).

The Criminal Intelligence Systems Operating Policies place the responsibility upon those operating the system to establish reasonable suspicion of criminal activity through information obtained from a participating agency or to a trained agency subject to inspection and audit (28 CFR § 23.20 (c)). The regulations also address the proper dissemination of information. "A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity" (28 CFR § 23.20 (e)).

The Privacy Act of 1974, the E-Government Act of 2002, and Title 28 Part 23 of the Code of Federal Regulations each address the manner in which information should be collected, maintained, and disseminated by government agencies. Adherence by fusion centers to the principles contained in these legislative acts aids in the protection of privacy rights—rights that have been well established in various U.S. Supreme Court cases throughout the years. This thesis proposes a decision-making model that melds privacy principles established by case law and the federal statutes. Fusion-center operators employing such a model would ensure consistency and coherency in implementing fusion-center guidelines established by DHS and DOJ.

B. CASE STUDIES

The table below illustrates a comparison between the privacy policies of the Chicago Police Department (CPD), California's State Terrorism Threat Assessment System (STTAS), and the Miami-Dade Police Department's (MDPD) Homeland Security Bureau (HSB).

Table 1. Privacy Policies Comparison

	Chicago CPIC	California STTAS	Miami-Dade HSB
Privacy Principles	**X**	**X**	**X**
Mission Statement		**X**	**X**
Reasonable Suspicion	**X**	**X**	**X**
MOUs	**X**	**X**	**X**
Training		**X**	**X**
Privacy Officer		**X**	
Info Retention		**X**	
Complaints		**X**	

1. Chicago Fusion Center Privacy Policy

A copy of Chicago's Crime Prevention and Information Center privacy policy can be found in Appendix A. As illustrated in Table 1, the policy addresses each of the eight fair information principles: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) openness; (7) individual participation; and (8) accountability, as recommended in the Fusion Center Guidelines (USDHS & DOJ, 2006). However, the policy does not include a specific mission statement, a specific section on training, or the designation of a privacy officer. Nevertheless, the policy does specify that participants in the center sign on to a memorandum of understanding to abide by the policy. Moreover, "information obtained from or through the CPIC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act" (Chicago Police Department, 2009, p. 2). This amounts to a requirement of reasonable suspicion of criminal activity.

2. California's Fusion Center Privacy Policy

California requires adherence to its State Terrorism Threat Assessment System Information Privacy Policy by each fusion center operating in California, including that in Los Angeles. A copy of this privacy policy is given in Appendix B. California's policy

is the most comprehensive. In addition to addressing the eight privacy principles, it includes a mission statement, detailed training requirements, designation of a privacy officer, and detailed instructions as to retention of information and complaints. Suspicious Activity Report information is particularly addressed:

> All SAR information will be reviewed for retention annually. At the end of one year, SAR information must be either purged or converted into criminal intelligence files, if the information satisfies the requirements for submission into criminal intelligence files. SAR information may be retained if, at a minimum, all personally identifiable information (or privacy field information) is removed and purged. (California, 2009, p. 17)

3. Miami-Dade Fusion Center Privacy Policy

The Miami-Dade Police Department operates the Homeland Security Bureau fusion center. A copy of its privacy policy can be found in Appendix C. Like Chicago and California, Miami-Dade includes the eight fair information principles. Furthermore, like California it specifically includes a detailed mission statement. However, it does not specifically cite a privacy officer, retention of information, or a complaint procedure.

4. Comprehensive Policy Model

Although all three policies specifically address the fair information principles, the California STTAS privacy policy is the most comprehensive of the three. Its policy covers the following fusion centers throughout California: 1) the Los Angeles Joint Regional Intelligence Center, 2) the Northern California Regional Intelligence Center, 3) the California State Terrorism Threat Assessment Center, 4) the Central California Intelligence Center, and 5) the San Diego Law Enforcement Coordination Center. The development of one policy for five centers resulted in the comprehensive privacy policy needed to address the concerns of multiple centers. Some of these concerns, such as information retention and complaints, are not addressed in the Chicago and Miami-Dade policies. The California model ensures consistency and coherence of fusion-center operations in regard to privacy and demonstrates how one policy can be utilized by

multiple centers. Similarly, a comprehensive policy designed to address privacy concerns at all fusion centers is possible. This thesis proposes such a policy.

C. GOVERNANCE STRUCTURE AND TRANSPARENCY ISSUES

The concerns of the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center illustrate the concerns that many citizens have regarding fusion centers. These concerns relate primarily to complex governance structures and a lack of transparency. Recommended policies must adequately address these concerns in order to protect privacy rights while facilitating fusion-center operations.

1. American Civil Liberties Union Concerns

In 2007, the American Civil Liberties Union released a report entitled, "What's Wrong with Fusion Centers?" The report, prepared by Michael German and Jay Stanley (2007), identified five areas of concern:

- Ambiguous lines of authority;
- Private sector participation;
- Military participation;
- Data mining;
- Excessive secrecy.

These areas of concern address issues of governance structures and transparency. According to the ACLU, the participation by multiple agencies in fusion centers permits agencies to avoid adherence to their own policies by requesting another participating agency to take action that is prohibited to them. This results in policy shopping (German & Stanley, 2007). Responsibilities are not clearly delineated. As such, the public is unsure to whom questions or matters of redress should be directed. Lines of authority are obscured.

Another area of concern for the ACLU arises from the participation of private, nongovernmental agencies in fusion centers. According to German and Stanley (2007),

such participation jeopardizes citizens' privacy. Nongovernmental agencies may be privy to the personal information of citizens—information to which they would not have access without participation in a fusion center. In addition, according to the ACLU, private agency participation presents an opportunity for government actors to hide illegal or questionable actions by requesting private agencies to perform activities that government agencies would be prohibited from performing. Also at issue is the delineation of responsibilities to these private agencies. Their place in the governance structure of a fusion center remains ambiguous at best.

A third area of concern identified by German and Stanley is military involvement in fusion centers. The National Guard participates in a number of fusion center operations. The ACLU acknowledges its fear that military participation enhances the probability that "officials who regard American communities as battlegrounds in a 'war' can be tempted to dispense with 'inconvenient' checks and balances" (German & Stanley, 2007, p. 15).

The ACLU maintains that data fusion is the equivalent of data mining (German & Stanley, 2007). Moreover, the agency contends that the DOJ guidelines for fusion center operations encourage data mining (German & Stanley, 2007). The agency's report, "What's Wrong with Fusion Centers?" states that the following will result from the data-mining activities of fusion centers:

> Many innocent individuals will be flagged, scrutinized, investigated, placed on watch lists, interrogated or arrested, and possibly suffer irreparable harm to their reputation, all because of a hidden machinery of data brokers, information aggregators and computer algorithms.
>
> Law enforcement agencies will waste time and resources investing in high-tech computer boondoggles that leave them chasing false leads—while real threats go unaddressed and limited resources are sucked away from the basic, old-fashioned legwork that is the only way genuine terror plots have ever been foiled. (German & Stanley, 2007, p. 15)

The final area of concern for the ACLU is their claim of excessive secrecy practiced by fusion centers. German and Stanley (2007) contend that such a practice prevents those injured by fusion centers to adequately seek redress. Furthermore, it

impedes the very mission of the fusion center—to prevent terrorism via information sharing. According to the ACLU, over-classification of documents and other materials is the unfortunate result of such excessive secrecy. The 9/11 Commission acknowledged the need for a new information-sharing system. “A decentralized network model, the concept behind much of the information revolution, shares data horizontally too. Agencies would still have their own databases, but those databases would be searchable across agency lines. In this system, secrets are protected through the design of the network and an ‘information rights management’ approach that controls access to the data, not access to the whole network” (9/11 Commission, 2004, p. 418).

In 2008, German and Stanley released an update to “What’s Wrong with Fusion Centers?” entitled “Fusion Center Update.” This update claimed that recent events had confirmed their worst fears as identified in the initial report. Law enforcement agencies monitored everyday, noncriminal behavior. Police officers were operating as national domestic intelligence agents. Fusion centers substantially increased data collection efforts. According to the ACLU, the population was moving swiftly toward a total surveillance society (German & Stanley, 2008).

According to German and Stanley, the Los Angeles Police Department issued a department directive requiring officers to report 65 behaviors, including “innocuous, clearly subjective, and First Amendment protected activities” (2008, p. 2). The collection of noncriminal information violates 28 CFR, Part 23 according to the ACLU (German & Stanley, 2008).

Another aspect that the ACLU warned against was the expansion of data-collection activities by fusion centers. According to German and Stanley, “The Washington Post reported in April of 2008 that fusion centers have increasing access to Americans’ private information through an array of databases. In addition to access to FBI and even CIA records, fusion centers often have subscriptions with private data brokers such as Accurint, Choice Point, Lexis-Nexus, and LocatePlus, a database containing cellphone numbers and unpublished telephone records” (German & Stanley, 2008, p. 3). The ACLU update report also cites examples in Pennsylvania and

Massachusetts, in which these state fusion centers bought credit reports and insurance-claim information ,respectively (German & Stanley, 2008).

Lastly, another area of concern identified by the ACLU is the use of fusion centers to collect information concerning peace activists and political dissenters (German & Stanley, 2008). According to the ACLU update report, the Maryland State Police monitored the activities of a well-known peace activist and shared his identifying information with a number of different agencies. The information was subsequently loaded into a database accessible to Maryland's fusion center—–the Maryland Coordination and Analysis Center. According to German and Stanley, the aforementioned incident is a prime example of "mission creep" by fusion centers, i.e., altering their focus from terrorism to political activities (2008).

2. Electronic Privacy Information Center Concerns

In September of 2007, Lillie Coney, the Associate Director of the Electronic Privacy Information Center (EPIC), appeared before the Data Privacy and Integrity Advisory Committee of the Department of Homeland Security. Coney expressed EPIC's concerns about fusion centers. In particular, Coney noted that "EPIC concluded that intelligence fusion center development and implementation is unfocused and undirected. The appropriate supervision, guidance and oversight necessary to assure privacy, civil liberty, and civil rights protection are imperative. Information fusion centers present grave threats to privacy and civil liberties" (Coney, 2007, p. 9).

Coney made six recommendations affecting the operation of fusion centers:

- DHS should identify the location, jurisdiction, and federal funding remitted to each fusion center;
- Funding should be dependent upon a federal privacy impact analysis;
- The Inspector General should investigate fusion centers' compliance to due process, privacy, civil liberties, and civil rights laws;
- Fusion centers should publicize the names of all its participants;

- Fusion centers should release annual reports concerning arrests, prosecutions, and convictions;
- Fusion centers should comply with the provisions of the Privacy Act of 1974 (5 USC § 552a) unless state statutes provide stronger protection, in which case, state statutes would apply.

It should be noted that in December of 2009, DHS instituted a policy in which fusion centers are to submit their privacy policies for review in order to receive funding. "Under the DHS grant guidelines, fusion centers must certify that their privacy and civil liberties protections are as comprehensive as the ISE Guidelines within six months of the grant award. To make this certification, the fusion centers must have had their privacy policies reviewed and on file with the ISE Privacy Guidelines Committee" (Geiger, 2009). However, once the grant award is made, no process is in place to halt funding if a fusion center violates its privacy policy. More than eighty percent of fusion centers have submitted privacy policies for review (ISE, 2010).

3. Addressing ACLU and EPIC Concerns

The primary objection to ACLU and EPIC concerns is that imposition of strict policies to prevent data mining and information sharing with private entities (or the military) and increase transparency hinders the ability of fusion centers to prevent terrorist or other criminal acts. The purpose of fusion centers is to facilitate information sharing among its participants, i.e., state, local, federal, or private partners. The premise is that, as a result of this information sharing, terrorist or other criminal incidents may be avoided. The proposed options examined by this thesis offer restrictions that satisfy the ACLU and EPIC concerns and promote consistency and coherence of fusion centers' policies, while simultaneously permitting the facilitation of information sharing.

III. PROPOSED OPTIONS

A. ESTABLISHING MANDATORY DEPARTMENT OF JUSTICE AND DEPARTMENT OF HOMELAND SECURITY PRIVACY GUIDELINES

In order to address the governance and transparency issues identified by the ACLU and EPIC, several options are available. One such option is to require mandatory implementation of DOJ and DHS guidelines.

1. Best Practices Utilizing DHS and DOJ Guidelines

In State Fusion Center Processes and Procedures: Best Practices and Recommendations, Rollins and Connors provide 12 recommendations for improving the establishment, support, and operation of fusion centers. As to the establishment of a fusion center, the authors recommend the development of a mission statement, strategies, policies and procedures, and a realistic budget spanning a number of years (Rollins & Connors, 2007). It is recommended that the various participants of the fusion center contribute to the development of these fundamentals. Moreover, the rules, responsibilities, and chain of command should be clearly delineated. Furthermore, "protection of privacy and civil liberties; the requirement as delineated in 28 CFR, part 23 should be addressed specifically" (Rollins & Connors, 2007, p. 6).

As to the supporting structure of a fusion center, Rollins and Connor recommend that two forms of governance structures be implemented: internal and external. The internal governance structure is comprised of entities that rely on the products and services of the fusion center. The external governance structure includes groups such as civil rights advocates. These members of governance committees ensure review and accountability. In addition to the internal and external governance structures, Rollins and Connors recommend the implementation of a staffing plan, memorandums of agreement, and education and training programs. Lastly, they recommend the use of templates, information-sharing policies and procedures, information technology structure, and security measures.

2. Federal Regulation Pros and Cons

Imposing the best practices identified by Rollins and Connors (2007) has its benefits and drawbacks. As a benefit, standardized implementation of guidelines would increase the consistency among fusion-center operations. It would lessen the likelihood of "policy shopping" as identified by the ACLU. Moreover, mandatory guidelines would strengthen the coherence of fusion centers by the public. Fusion-center policies would be clearer and less confusing to the public because they would be less likely to differ from center to center. Because the guidelines would be mandatory, it would strengthen the ability of DHS to grant funding to those centers who met the guidelines. Such an arrangement would serve as a deterrent for fusion centers to violate citizens' privacy. Violation of citizens' privacy would amount to violation of the guidelines, which would result in no funding from DHS.

As a drawback to mandatory implementation of guidelines, fusion centers would be less likely to be innovative in addressing hazards unique to their own regions for fear of losing DHS funding. One set of standards applied to the establishment, support, and operation of all fusion centers may not be appropriate in all circumstances. Implementation of mandatory guidelines may increase confusion and lead to less coherence where state laws differ from federal laws regarding privacy. The problem with "one size fits all" is that oftentimes one policy does not fit in all circumstances. Fusion centers may then be forced to implement a list of exceptions to policies that undermine the very principles the guidelines seek to uphold: 1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards; 6) openness; 7) individual participation; and 8) accountability (USDHS & DOJ, 2006).

B. UTILIZING A BALANCING TEST AND ADMINISTRATIVE REVIEW PROCESS

Another available option to address the governance and transparency issues identified by the ACLU and EPIC is the use of a balancing test and administrative review process. The balancing test would encompass the elements of reasonable expectation of privacy identified in *Katz* and the exigent circumstances principle.

1. Elements of the Balancing Test

Criminal law regularly utilizes balancing tests to assess law enforcement action. Two well known tenets of criminal law are the "reasonable expectation of privacy" and "exigent circumstances." An analysis of those tenets would address the appropriateness of their application to fusion-center activities. The proposed balancing test would be comprised of two prongs: 1) assessment of the extent to which citizens possess the reasonable expectation of a right to privacy as to the information in question, and 2) existence of exigent circumstances requiring immediate action as to the information in order to prevent serious physical harm or death. In cases where no reasonable expectation of privacy exists, as explained in *Katz*, fusion centers could collect or disseminate the information. In cases where a reasonable expectation of privacy exists, but exigent circumstances also exist that could result in imminent serious bodily harm or death, information could also be collected or disseminated.

2. Administrative Review Process

In cases wherein citizens possess a reasonable expectation of privacy and no exigent circumstances exist, an administrative review process would be required prior to the collection, maintenance, or dissemination of the information by a fusion center. An individual or committee higher in authority than the functional operators of the fusion center would decide whether the citizen's right to privacy outweighed the fusion center's need to collect, maintain, or disseminate the information. Because no exigent circumstances exist, time is available for a more in-depth review prior to taking one of the aforementioned actions. In the event that no reasonable expectation of privacy exists, review beyond the functional operators of the fusion center is not required. If a reasonable expectation of privacy and exigent circumstances exist, functional operators would also decide on the propriety of collecting, maintaining, or disseminating the information when little or no time is available for further review.

3. Pros and Cons of Balancing Test and Administrative Review

Requiring a balancing test and administrative review would result in a more consistent and coherent application of the DHS and DOJ guidelines as all fusion centers would implement this policy. However, the speed by which information flowed would be impaired in those cases requiring an administrative review. As not all information is known, exigent circumstances could exist of which fusion center operators would not be aware. Administrative review would reduce the center's ability to disseminate information in a timely manner, thereby causing the center to unknowingly exacerbate a dangerous situation.

C. IMPOSING A REASONABLE-SUSPICION REQUIREMENT

The final option analyzed by this thesis is the reasonable-suspicion requirement. Such a requirement is quite familiar to law enforcement agencies as it plays an important role in their daily activities, i.e., stopping and searching individuals suspected of committing a crime. Application of the requirement to the collection, maintenance, and dissemination of information within the context of a fusion center, then, is very feasible.

1. Definition of Reasonable Suspicion Under Criminal Law

The reasonable suspicion requirement was established in *Terry v. Ohio* (1968). The United States Supreme Court stated that "it is necessary 'first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen,' for there is 'no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails'… And in justifying the particular intrusion the police officer must be able to point to articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion" (*Terry v. Ohio*, 392 U.S. 1, 21–22 (1968)).

2. Application of Reasonable Suspicion Requirement to Fusion Centers

The Code of Federal Regulations also requires that reasonable suspicion of criminal activity exist prior to collecting, maintaining, or disseminating information. An operating agency must be able to articulate that the facts indicate rational inferences of a crime. According to 28 CFR § 23.20 (c), "Reasonable suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise."

3. Pros and Cons of a Reasonable Suspicion Requirement

The imposition of a reasonable-suspicion requirement serves to protect citizens' privacy by limiting the collection of their personal information by a law enforcement agency. Without a nexus to criminal activity, law enforcement is free to collect and store information without restraint. Such information could be utilized to chill the exercise of First Amendment activities by citizens.

In addition, the reasonable-suspicion requirement does not necessitate an agency's obtaining a warrant to collect information. While limiting law enforcement's actions in some regard, the reasonable-suspicion requirement also facilitates its activities in the collection of information by satisfying the Fourth Amendment—not engaging in unreasonable searches and seizures—without going through the complicated process of obtaining a warrant.

Though the reasonable-suspicion requirement helps to protect citizens' privacy and satisfies the Fourth Amendment, the limitation of information tied to criminal activity serves to restrain law enforcement's capabilities to "connect the dots." Some information when viewed on its own appears innocuous but when viewed in relation to other information may be an indication of something more important. In addressing terrorism a fusion center's ability to piece together various fragments of information may affect an agency's capacity to prevent a terrorist incident.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CHOOSING THE RIGHT POLICY

In deciding which policy to recommend, it is best to judge the proposed courses of action by their impact on consistency and coherence of governance structures and transparency. Both variables are equally important to the protection of the public's right to privacy. The recommended policy must be simple to apply and provide a consistent method for protection of privacy rights. Furthermore, the recommended policy must afford a coherent view of the fusion center's governance structures (defined roles, delineated responsibilities, and accountability) in order to ensure that, should fusion centers fail to adhere to privacy policies, the public is alerted as to what corrective action it should take. In The Privacy Challenges of U.S. Fusion Centers, Andino (2008) identified several assessment areas as to transparency: openness, collection, use, individual participation, and accountability. Utilizing these assessment areas will provide a comprehensive analysis of the proposed policies. The matrix below provides a comparative analysis of the proposed options as to governance structure and transparency. The number "1" indicates little or no positive impact. The number "3" indicates medium positive impact. Lastly, the number "5" indicates high positive impact.

Table 2. Comparison Matrix of Proposed Options

Variables*	**Mandatory Guidelines Option**	**Balancing Test & Administrative Review Option**	**Reasonable Suspicion Option**
Defined Roles	5	5	1
Delineated Responsibilities	5	5	1
Accountability	5	5	1
Openness	3	3	1
Collection	5	5	5
Use	5	5	5
Individual Participation	3	3	1

* Governance encompasses defined roles, delineated responsibilities, and accountability. Transparency encompasses openness, collection, use, and individual participation.

A. MANDATORY DOJ AND DHS GUIDELINES OPTION

As indicated in the table above, the imposition of mandatory guidelines would highly impact governance structures. Mandatory rules and procedures require defined roles for participants with clearly delineated responsibilities for all. Moreover, participating persons and agencies may be held accountable for performing their responsibilities.

On the other hand, mandatory guidelines have medium effect upon some aspects of transparency, i.e., openness and individual participation. Mandatory guidelines do, however, greatly impact the collection and use of information. The effect depends greatly upon instituting mandatory rules and procedures, making certain aspects of the fusion center transparent to the public, and enforcing these rules and procedures. Even with mandatory guidelines in place, fusion centers may allow agencies to utilize partnerships with other agencies to circumvent the guidelines. If the fusion center does not own the data, even though they view it and analyze it, the center does not comply with FOIA requests.

B. BALANCING TEST AND ADMINISTRATIVE REVIEW OPTION

The balancing test and administrative review option, like the mandatory guidelines option, has a significant impact on the governance structures. The test is coherent in its application since law enforcement agencies are already familiar with reasonable-expectation-of-privacy principles. Specific, higher approval by administrative review would be required for the collection and use of personal information in which a reasonable expectation of privacy existed and no exigent circumstances were evident in which serious bodily harm or death was imminent. However, this decision-making apparatus has medium impact on openness to the public and individual participation by the public. The decision-making tools (balancing test and administrative review) are all in-house, under the fusion center's control.

C. REASONABLE-SUSPICION OPTION

As indicated above, the reasonable-suspicion option has the highest degree of impact as to collection and use of data. As a decision-making tool, it aids fusion-center operators in choosing what information to collect and store using the center's criminal intelligence systems, as required per 28 CFR, Part 23. However, the public remains in the dark about specifically what information is being collected and used by fusion centers. Furthermore, the reasonable-suspicion requirement fails to define roles, delineate responsibilities, or address accountability issues. However, like the balancing test option of analyzing the existence of a reasonable expectation of privacy, law enforcement agencies are quite familiar with the principles of reasonable suspicion. Therefore, its application is coherent and can be consistently applied.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE RECOMMENDED POLICY

This thesis recommends imposing all three of the aforementioned options: mandatory guidelines, a balancing test and administrative review, and a reasonable-suspicion requirement. As illustrated by Table 2, each policy on its own is deficient in that it fails to adequately address each governance structure and transparency issue. However, a combination of the three accomplishes that task.

A. MANDATORY FUSION CENTER GUIDELINES

First, it is clear that guidelines alone without a requirement that they be imposed leads to inconsistency in application of the guidelines from fusion center to fusion center. Not all guidelines need to be mandatory. However, those that directly affect the privacy rights of citizens and, therefore, have constitutional implications, must be mandatory. The DHS has recognized this fact and required fusion centers to submit their privacy policies for review in order to receive DHS funding (Geiger, 2009). Therefore, it is recommended that the DOJ and DHS fusion center guidelines be mandatory.

B. MANDATORY BALANCING TEST AND ADMINISTRATIVE REVIEW POLICY

Secondly, in order to further protect the personal information of citizens, it is recommended that fusion centers mandatorily utilize a balancing test and administrative review process when deciding to collect or disseminate information. The balancing test has two prongs: 1) ascertain whether a reasonable expectation of privacy exists and 2) ascertain whether exigent circumstances exist in which serious bodily harm or death to person(s) is imminent. Administrative review of higher authority beyond that of fusion center operators and analysts would be required where a reasonable expectation of privacy existed and no exigent circumstances were evident.

C. MANDATORY REASONABLE SUSPICION REQUIREMENT

Thirdly, it is recommended that all fusion centers collect and maintain information only if reasonable suspicion exists of criminal activity. The centers would not be able to circumvent 28 CFR Part 23 by failing to enter such information in criminal intelligence systems funded by federal grants. Nor would the centers be permitted to engage private sector (or public) partners to collect the information in the absence of a criminal investigation.

D. CONCLUSION

Fusion centers must balance citizens' privacy rights with the need to collect, analyze, and disseminate information to prevent terrorism and other crimes. The DOJ and DHS issued a number of guidelines to aid in this endeavor. However, because the guidelines are not mandatory, fusion centers vary in privacy policies and procedures.

The ACLU and EPIC identified a number of concerns relating to complex governance structures and lack of transparency. This thesis recommends the mandatory implementation of three policies in order to ensure consistency and coherence of operational structure and transparency in the implementation of policies by fusion centers; this will simultaneously guard against the abuse of privacy rights and facilitate the collection, analysis, and dissemination of information. Mandatory imposition of the DOJ and DHS fusion center guidelines, a balancing test and administrative-review process, and a reasonable-suspicion requirement would ensure coherent and consistent governance structures and transparency as to fusion centers, thereby striking the right balance between protecting citizens' privacy rights and permitting fusion centers to collect, analyze, and disseminate intelligence in the information-sharing era.

The examination of federal cases and statutes establishes that privacy is a fundamental, constitutional right. As such, all fusion centers should be required to impose the DOJ and DHS privacy guidelines in order to ensure uniform protection of this right. Furthermore, all fusion centers should restrict the collection of information to that related to criminal investigations established by the existence of reasonable suspicion of

criminal activity. Lastly, all fusion centers should ascertain whether a reasonable expectation of privacy exists when collecting or disseminating information. In the event that such an expectation exists and no exigent circumstances are present involving imminent death or serious physical injury to persons, administrative review of higher authority than the low- or mid-level operators of the fusion center would be required prior to the collection or dissemination of the information. However, where an expectation of privacy exists and exigent circumstances are present, low- or mid-level operators would unilaterally decide whether to collect or disseminate the information. Likewise, where no reasonable expectation of privacy is present, low- or mid-level fusion-center operators may collect or disseminate information as long as the reasonable suspicion requirement is met.

There is little or no additional financial costs associated with the implementation of these recommendations. Due to fusion centers' use of criminal intelligence systems and their dependence on federal funding, most fusion centers already require reasonable suspicion of criminal activity in order to ensure compliance with 28 CFR Part 23. The use of a test balancing citizens' reasonable expectations of privacy against the fusion center's need to collect, analyze, and disseminate information and the use of an administrative review process also carry little or no additional costs as the structures are already in place via command-channel review in law enforcement agencies, which operate many of the fusion centers.

As fusion centers' policies become more standardized, more focus should then be placed upon the efficacy and efficiency of these policies and whether the centers facilitate information sharing to such a degree as to contribute significantly to the prevention of terrorism or other crimes. But for now, the imposition of mandatory policies and standards designed to protect citizens' privacy should be the primary focus.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CHICAGO POLICE DEPARTMENT'S CRIME PREVENTION AND INFORMATION CENTER PRIVACY POLICY

CRIME PREVENTION AND INFORMATION CENTER PRIVACY POLICY

The **Crime Prevention and Information Center** is a Fusion Center (herein referenced to as **"CPIC"** as defined below:

The CPIC project was initiated in response to the increase need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of CPIC focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

CPIC's intelligence products and services will be made available to law enforcement agencies and other criminal justice entities. All agencies participating in the CPIC will be subject to a Memorandum of Understanding and will be required to adhere to all CPIC's policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

GUIDING PRINCIPLES

CPIC's Privacy Policy embraces the eight Privacy Design Principles which shall guide the policy and practices wherever applicable. The eight Privacy Design principles are:

1. **Purpose Specification** – Define the CPIC's purpose for information to help ensure the agency's use of information is appropriate.
2. **Collection Limitation** – Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality** – Ensure data accuracy.
4. **Use Limitation** – Ensure appropriate limits on Department use of personal information.

5. **Security safeguards** – Maintain effective security over personal information.
6. **Openness** – Maintains a citizen access to information available through the Freedom of Information Act.
7. **Individual Participation** – Allow individual's reasonable access and opportunity to correct errors in their personal information held by the Agency.
8. **Accountability** – Identify, train and hold agency personnel accountable for adhering to agency information quality and privacy policies.

I. Purpose Specification

CPIC has developed databases by using existing data sources from federal, state and local law enforcement to integrate data with the goal of identifying, developing and analyzing intelligence related to violent crimes, terrorist activity and other crimes for investigative leads**.** This capability will facilitate integration and exchange of information between participating law enforcement agencies.

II. Collection Limitation

The CPIC is maintained for the purposes of developing information and intelligence by agencies who participate in the CPIC. The decision of an agency to participate in CPIC and about which databases to provide is voluntary. Information obtained and disseminated by a law enforcement agency outside of Chicago will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal laws..

Because the laws, rules or policies governing information and intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Therefore, each contributor of information is under different legal restraints and restrictions. Each agency has its own responsibility to abide by the collection limitations applicable

to it by reasons of law. Information contributed to the center should be that which has been collected in conformance with those limitations.

III. Data Quality

The agencies participating in the Crime Prevention and Information Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

IV. Use Limitation

Information obtained from or through the CPIC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

The primary responsibility for the overall operation of the Crime Prevention and Information Center will be the Commander of the Deployment Operations Center of the Chicago Police Department. The Commander will enforce the Privacy Policy of the CPIC and take the necessary measures to make certain that access to the CPIC's information and resources is secure and will prevent any unauthorized access or use. The Chicago Police Department reserves the right to restrict the qualifications and number of personnel who will be accessing CPIC and to suspend or withhold service to any individual violating this Privacy Policy. The Department, or persons acting on behalf of the Department, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

Security for information derived from CPIC will be provided in accordance with all applicable federal, state and local laws, the rules and regulations of the Chicago Police Department, and CPIC policies. Furthermore, all personnel who receive, handle, or have access to CPIC data and/or sensitive information will be trained as to those requirements. All personnel having access to the CPIC's data agree to abide the following rules:

1. CPIC's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer and CPIC.
2. Individual passwords will not be disclosed to any other person except as authorized by the Department.
3. Individual passwords will be changed if authorized personnel of the Department, the CPIC or any individual password holder suspects the password has been improperly disclosed or otherwise compromised.
4. Background checks will be completed on personnel who will have direct access to CPIC.
5. Use of CPIC's data in an unauthorized or illegal manner will subject the user to denial of further use of the CPIC; discipline by the user's employing agency, and /or criminal prosecution.

Each authorized user understands that access to the CPIC can be denied or rescinded for failure to comply with the application restrictions and use limitations.

V. Security Safeguard

Information obtained from or through the CPIC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3)

disseminated to unauthorized persons.

Use of CPIC's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the CPIC will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening process using procedures and standards established by Chicago Police Department. Each individual user must complete and Individual User Agreement in conjunction with training.

The Crime Prevention and Information Center operates in a secure facility, protecting the CPIC from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions. Access to CPIC databases from outside the facility will only be allowed over secure networks. The CPIC will store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such action.

VI. **Openness**

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation. CPIC is a collection of various databases, which allows the Department and participating agencies to share information and to accelerate the dissemination of information already collected. CPIC does not change or alter a citizen's rightful access to information accorded to them under state law. The CPIC will post the Privacy Policy on the premises of the CPIC and make it available to any interested party.

VII. Individual Participation

The data maintained by CPIC is provided, on a voluntary basis, by the

participating agencies or is information obtained by other sources. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretations, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the CPIC's applications. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question. Participating agencies agree that they will refer requests related to privacy or sunshine laws back to the originator of the information.

VIII. Accountability

When a query is made to any of the CPIC's data applications, the original request is automatically logged by the CPIC's **Event Manager Statistical Electronic Log** system which will identify the user initiating the query. When such information is disseminated outside the agency from which the original request is made, a second dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency

for law enforcement investigative purpose or other agencies as provided by law.

The agency from which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

1. Date of release
2. To whom the information relates
3. To whom the information was released (including address and telephone number)

4. All identification numbers or other indicator that clearly identifies the data released

5. The purpose for which the information was released

The Chicago Police Department will be responsible for conducting or coordinating audits and investigating misuse of CPIC's data or information. All violations and/or exceptions shall be reported to the *Chicago Police Department Deployment Operations Center.* Individual users of the CPIC's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use of limitations for the use of CPIC's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the CPIC is required to abide by this *Privacy Policy* in the use of information obtained by and through the Chicago Police Department's CPIC.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. CALIFORNIA'S FUSION CENTER PRIVACY POLICY

STATE TERRORISM THREAT ASSESSMENT SYSTEM
INFORMATION PRIVACY POLICY

Each of the fusion centers which comprise California's State Terrorism Threat Assessment System (STTAS) have individually and, collectively, committed their center to comply with Title 28, Code of Federal Regulations Part 23, the National Strategy For Information Sharing, applicable national guidelines developed by the United States Department of Justice through the DOJ-sponsored Global Justice Information Sharing Initiative and the Department of Homeland Security Advisory Council, and the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files and Criminal Intelligence Operational Activities. The signatures below reflect this ongoing commitment and approval of the STTAS Information Privacy Policy as a baseline set of standards and principles that apply throughout the STTAS. While each of the STTAS components retain the discretion to implement a privacy policy for each center or agency, those policies will adhere to the principles and standards articulated within this Policy. This Policy shall be reviewed annually and updated as appropriate with the concurrence of each signatory.

9/22/09
Executive Director Leslie Gardner — DATE
Los Angeles Regional Intelligence Center

10-14-09
Director Ronald E. Brooks — DATE
Northern California Regional Intelligence Center

10/19/2009
STTAC Commander Kyle Scarber — DATE
State Terrorism Threat Assessment Center

10/14/2009
Director Timothy Johnstone — DATE
Central California Intelligence Center

9/16/09
RTTAC Commander Lee Yoder — DATE
San Diego Regional Terrorism Threat Assessment Center

John R. Kingston, SD-LECC — 9/16/09
JOHN R. KINGSTON, DIRECTOR

California
State Terrorism Threat Assessment System
Information Privacy Policy

Mission:

The California State Terrorism Threat Assessment System (STTAS) is a collaborative effort to lawfully and appropriately gather and analyze information, employ analytical tools and methodologies to produce and share timely and actionable homeland security information between agencies and across the full range of public safety disciplines. The STTAS consists of four Regional Terrorism Threat Assessment Centers (RTTACs) and a single state-wide center: the Northern California Regional Intelligence Center; the Los Angeles Joint Regional Intelligence Center; the San Diego Law Enforcement Coordination Center; the Central California Intelligence Center; and, California State Terrorism Threat Assessment Center (STTAC).(Hereinafter collectively referred to as "STTAS Components".)

Policy Applicability and Legal Compliance

The STTAS Information Privacy Policy ("Privacy Policy") provides authoritative guidance, direction and establishes the policies and procedures regarding the manner in which information is collected, received, maintained, archived, accessed, or disclosed within the STTAS, and disclosed to other governmental entities, private contractors, and the general public.

The Privacy Policy applies to information about individuals and organizations obtained by the STTAS in furtherance of its analytical mission. Information which furthers an administrative or other non-analytical purpose (such as personnel files, or information regarding fiscal, regulatory or other matters associated with the operation of the STTAS as governmental entities) or which does not identify an individual or organization will be handled in a manner which complies with all applicable privacy laws and regulations but will not be subject to the provisions of this policy.

The STTAS, and all assigned or detailed personnel, shall comply with all laws and regulations that govern the handling of national security classified information. This policy does not apply to national security classified information.

The STTAS, and all assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in any STTAS Component, shall comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. The internal operating policies of each STTAS Component will be consistent with this Privacy Policy and will incorporate applicable laws protecting privacy, civil rights, and

civil liberties. The desired outcome of this policy is to protect the privacy rights of US persons. Each STTAS Component has adopted this Privacy Policy as an internal operating policy and implements it, and other necessary policies, in a manner consistent with the U.S. Constitution, California Constitution, the Intelligence Reform and Terrorism Prevention Act, 28 CFR Part 23, the California Public Records Act and the California Information Practices Act of 1977.

Retaining Information

What Information May Be Retained?

STTAS Components will not retain information that was not collected in a lawful manner. STTAS Components will comply with 28 C.F.R. Part 23, the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files (CA AG's Guidelines) and the California Constitution and, with regard to the State Terrorism Threat Assessment Center (STTAC), the California Information Practices Act (Gov. Code § 1798 et seq.).

All STTAS Components may only place information in criminal intelligence files and/or retain information:

1. Where there is reasonable suspicion that a specific individual or organization has committed or is supporting or facilitating a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, California, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity; or,

2. Where there is a reasonable likelihood that within one year there will develop a reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, California, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.

3. That is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be filed and retained provided that (1) the information is labeled as "Non-Criminal Identifying Information"; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal (including terrorist) activity; and, (3) the individual or organization which is the criminal suspect identified by this information otherwise meets all requirements of 28CFR Part 23. We are mindful of the recommendation within the CA AG's Guidelines that such information not be included in criminal intelligence files. It is imperative

that, where it is determined to be necessary to support authorized analytical or investigative activity, non-criminal identifying information be clearly labeled as such to ensure that the subject of the information is not inappropriately connected to criminal activity.

4. That is useful in a crime or threat analysis or otherwise in furtherance of the public safety, anti-terrorism, counter-terrorism, or homeland security responsibilities of the STTAS and its components; provided that the source of the information is reliable or limitations on the quality of the information have been identified.

5. Such as tips, leads, or suspicious activity reports, which is based on mere suspicion of criminal (including terrorist) activity that falls within the public safety, anti-terrorism, counter-terrorism, or homeland security responsibilities of the STTAS and each component fusion center.

STTAS Components will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or his or her race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

1. Relevant to whether an individual or organization has engaged in, is engaging in, or is planning criminal (including terrorist) activity; or

2. Needed by the agency:

    i) To identify an individual,
    ii) In order for the agency to operate effectively, or
    iii) To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

Information that shall be specifically excluded from criminal intelligence files includes:

a. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.
b. Information on an individual or group merely on the basis of race, gender, age, or ethnic background.
c. Information on an individual or group merely on the basis of religious or political affiliations or beliefs.
d. Information on an individual or group merely on the basis of personal habits and/or predilections that do not violate any criminal laws or threaten the safety of others.

e. Information on an individual or group merely on the basis of involvement in expressive activity that takes the form of non-violent civil disobedience that amounts, at most, to a misdemeanor offense.

Methods of Seeking or Receiving Information

(a) The primary sources of information to each STTAS Component are other governmental entities, including the member organizations that comprise each Component (through various information systems operated by governmental entities, and through searches of publicly available records, particularly those accessible through the Internet). Information gathering techniques used by this agency will comply with all applicable laws.

(b) STTAS Components will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider if the agency knows or has reason to believe that the individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the agency.

(c) STTAS Components will maintain a record of information sought and received.

(d) While the member organizations of each STTAS Component may have criminal investigative authorities and responsibilities, the STTAS Components, when acting as a fusion center, do not conduct investigations.

Classification of Information Regarding Validity and Reliability

(a) At the time of retention, the information will be categorized regarding it's:

1. Content validity;
2. Nature of the source;
3. Source reliability;
4. Accuracy;
5. Completeness; and,
6. Currency

(b) At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

1. Protect confidential sources and police undercover techniques and methods;
2. Not interfere with or compromise pending criminal investigations;
3. Protect an individual's right of privacy and civil rights;

4. Provide legally required protection based on the status of an individual as a victim or witness, as a child sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

(c) STTAS Component personnel will assess the information to determine its nature and purpose. Personnel will assign information to categories to indicate the result of the assessment, such as:

1. Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;
2. The nature of the source (for example, anonymous tip, interview, public records, private sector);
3. The reliability of the source (i.e., reliable, usually reliable, unreliable, unknown); and
4. The validity of the content (i.e., confirmed, probable, doubtful, cannot be judged).

(d) The categorization of retained information may be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

(e) STTAS Components shall keep a record of the source of information retained by that Component. In this context, "source" refers to the individual or entity which provided the information to the Component. If the source is an agency, governmental entity, or other organization, such as a corporation or association, this requirement can be met by maintaining the name of the agency, governmental entity, or organization, a long as the specific unit of that agency, governmental entity, or organization which provided the information is identified.

(f) These requirements do not apply to analytical products and other information obtained from or originated by a federal, state or local entity that has itself evaluated the validity and reliability of information in accordance with these principles or the conventions of the intelligence and law enforcement communities.

(g) STTAS Components will make reasonable efforts, including the use of appropriate contractual requirements, to ensure that information obtained from commercial databases was collected using lawful techniques. STTAS Components will contract only with commercial database entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable local, state and federal laws and that these methods are not based on misleading collection practices.

(h) Information which pertains to U.S. Persons or is subject to specific restrictions on access, use or disclosure will be marked appropriately.

Tips, Leads, and Suspicious Activity Reports

STTAS Components routinely receive tips, leads, or other reports of suspicious activities. Component personnel evaluate the information and, where appropriate, forward it to the Regional Terrorism Threat Assessment Advisory Center (RTTAC) or RTTACs with geographic responsibility for further evaluation or investigation of the tip, lead or report in accordance with applicable procedures and direction provided by the RTTAC leadership. Depending on the nature of the information, and particularly when credible information indicates a potential danger to life and property, the Component may report the information to CHP, Cal EMA and other governmental entities with law enforcement, counterterrorism, or national security responsibilities. The STTAC does not conduct investigative activity based on tips, leads or suspicious activity reports.

With regard to tips, leads, or suspicious activity reports, STTAS Component personnel will:

1. Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to distinguish it from other information;
2. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion;
3. Adhere to and follow the Component's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

STTAS Components will seek or retain information that a source agency has determined constitutes "suspicious activity" and which:

1. Is based on (a) a criminal predicate or (b) a possible threat to public safety; including potential terrorism-related conduct; and
2. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; or the prevention or crime; and
3. The source agency assures was acquired in accordance with agency policy and in a lawful manner.

STTAS Components will not retain suspicious activity report information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

Upon receipt of SAR information from a source agency, STTAS Component personnel will:

Personally review and vet the SAR information and make the appropriate assessment in accordance with guidelines governing the system within which the information is stored (such as ISE-SAR, e-Guardian, COPLINK etc.)
Ensure that any information posted to a SAR repository includes appropriate labels;
Notify the source agency of the disposition of the SAR information.

The STTAS component will ensure that certain basic and special descriptive information is entered and electronically associated with SAR information including:

1. The name of the source agency;
2. The date the information was submitted;
3. The point of contact information for SAR-related data; and
4. Information that reflects any special laws, rules or policies regarding access, use and disclosure.

Information provided in a SAR repository shall indicate, the maximum extent feasible:

1. The nature of the source: anonymous tip, confidential source; trained interviewer or investigator; written statement (victim, witness, other), private sector, or other source; and
2. Confidence, including:
    - The reliability of the source (reliable, unreliable or unknown); and
    - The validity of the content (confirmed, doubtful, or cannot be judged).
3. Due diligence will be exercised in determining source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
4. Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.

At the time a decision is made to post SAR information to an external SAR repository such as ISE-SAR, e-Guardian, or COPLINK, STTAS Component personnel will ensure that the information is labeled to the maximum extent feasible and consistent with applicable standards, to reflect any limitations on disclosure based on sensitivity of disclosure, in order to:

1. Protect an individual's right of privacy, civil rights, and civil liberties;
2. Protect confidential sources and police undercover techniques and methods;
3. Not interfere with or compromise pending criminal investigations; and

4. Provide any legally required protection based on an individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

STTAS Components will ensure that SAR information posted in an external repository that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.

STTAS Components will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR information into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the privacy, civil rights, and civil liberties of individuals.

Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the STTAS or a STTAS Component will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

When a choice of investigative techniques is available, information documented as a SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

Information Quality

A substantial portion of the information received by STTAS Components is in the form of completed analytical product. The STTAC does not use these products to conduct investigations or to support prosecutions but rather in furtherance of its mission to analyze and assess strategic threats to the state. The rigorous examination of information quality is a critical component of effective analysis. The member organizations of each RTTAC may use the information in furtherance of investigative or other activities within their jurisdiction and authority. However, STTAS Components are not responsible for providing feedback to other agencies regarding the analytical efforts or products of those

agencies simply because the Component may not concur with the analysis. While some feedback may occur, it need not be formal or routine.

(a) STTAS Components will make every reasonable effort to ensure that information sought or retained is:

1. Derived from dependable and trustworthy sources of information;
2. Accurate;
3. Current;
4. Complete, including the relevant context in which it was sought or received and other related information; and
5. Merged with other information about the same individual or organization only when the applicable standard has been met.

(b) STTAS Components will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

(c) STTAS Components will actively research suspected errors and deficiencies and will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that:

1. The information is erroneous, misleading, obsolete, or otherwise unreliable;
2. The source of the information did not have authority to gather the information or to provide the information to the agency; or
3. The source of the information used prohibited means to gather the information.

(d) Originating agencies providing data remain the owners of the data contributed. STTAS Components will take reasonable steps to advise the appropriate data owner if its data is found to be inaccurate or incomplete where the Component is the primary or initial recipient of such information.

(e) STTAS Components shall maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness. Such standard need not be met except when such records are used to make any determination about the individual. When Component personnel transfer a record outside of the STTAS, the Component shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely. Each Component shall notify any recipient agency if information provided by the Component is determined to be inaccurate, incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the subject individual may be affected.

Collation and Analysis of Information

Collation and Analysis

(a) Information sought or received by the agency or from other sources will only be analyzed:

1. By qualified individuals who are authorized to access the information;
2. To provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist), activities generally; and
3. To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.
4. To create strategic, geographic region, or critical infrastructure sector, specific analysis products providing state, local and agency leadership with treat and risk assessment information upon which to base resource prioritization, information analysis and awareness decisions.

(b) Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates this policy. Only information which has been properly collected and retained may be analyzed.

SAR Information posted to the shared space or accessed from the shared spaces will be analyzed for intelligence purposes only by qualified personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved and trained accordingly (including training on the implementation of this policy). These personnel shall share SAR information only through authorized analytical products.

Merging of Information from Different Sources

(a) The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

(b) If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

Dissemination of Information

(a) STTAS Components will identify and review protected information that originated in the center prior to sharing that information in the ISE. Further, the center will provide notice mechanisms, including but not limited to metadata or data fields, that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

(b) In accordance with the Information Practices Act of 1977, the STTAC shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made pursuant to subdivision (i), (k), (l), (o), or (p) of Civil Code Section 1798.24. This accounting shall also be required for disclosures made pursuant to subdivision (e) or (f) of Civil Code Section 1798.24 unless notice of the type of disclosure has been provided pursuant to Civil Code Sections 1798.9 and 1798.10. The accounting shall also include the name, title, and business address of the person or agency to which the disclosure was made. For the purpose of an accounting of a disclosure made under subdivision (o) of Civil Code Section 1798.24, it shall be sufficient for the STTAC to record the date of disclosure, the law enforcement or regulatory agency requesting the disclosure, and whether the purpose of the disclosure is for an investigation of unlawful activity under the jurisdiction of the requesting agency, or for licensing, certification, or regulatory purposes by that agency. Routine disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement or regulatory agencies of federal, state, and local government shall be deemed to be disclosures pursuant to subdivision (e) of Civil Code Section 1798.24 for the purpose of meeting this requirement. STTAS Components other than the STTAC are not subject to the requirements of the Information Practices Act of 1977. The STTAC will assert all appropriate exemptions, including but not limited to Civil Code Section 1798.40.

The employees and users of the participating agencies and of the agency's information service providers will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. STTAS Components will include a statement substantially similar to the following in the transmittal documents when information is disseminated: "Receipt of this information constitutes acceptance of all terms and conditions regarding its use, handling, storage, further dissemination or destruction. At a minimum, receipt acknowledges a commitment to comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information."

SAR information submitted into an external SAR repository such as ISE-SAR or e-Guardian and retained by a STTAS Component will be accessed by or disseminated only to persons within the STTAS or, as expressly approved by the appropriate authority for the applicable SAR repository, to include users of the system who are authorized to have access and need the information for specific

purposes authorized by law. Access and disclosure of personal information will only be allowed to agencies and individual users which comply with the principles set forth in 28 CFR Part 23, need access to the information for legitimate law enforcement and public protection purposes and will use the information only for the performance of official duties in accordance with law.

Credentialed, role-based access criteria will be used, as appropriate, to control:

> The information to which a particular group or class of users can have access based on the group or class;
> The information a class of users can add, change, delete, or print; and
> To whom, individually, the information can be disclosed and under what circumstances.

Access to or disclosure of records will be provided only to persons within the STTAS Component or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. Agencies external to the STTAS Component may not disseminate information received from the Component without specific approval of the originator of the information.

Sharing Information with Those Responsible for Public Protection, Safety, or Public Health

(a) Information retained by Components may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

(b) Criminal intelligence information may be disseminated to law enforcement, homeland security, or counterterrorism agencies for any type of detective, investigative, preventive, or intelligence activity when the information falls within the law enforcement, counterterrorism, or national security responsibility of the receiving agency; or, may assist in preventing a crime or the use of violence or any conduct dangerous to human life or property; or, to officials within the U.S. Department of Justice Office of Justice Programs when they are monitoring or auditing the Component's compliance with 28 CFR Part 23. Participating agencies that access information from a STTAS Component must comply with any applicable dissemination limitations or practices imposed by the STTAS Component or the originator of the information. This may, or may not, include obtaining approval of the originator prior to further dissemination.

(c) Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid danger to life or property.

(d) An audit trail will be kept of the access by or dissemination of information to such persons.

Sharing Information for Specific Purposes

(a) Information gathered and retained by this agency may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

(b) An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

Disclosing Information to the Public

(a) Information gathered and retained by STTAS Components may be disclosed to a member of the public in accordance with the California Public Records Act, the Information Practices Act, or otherwise in a manner consistent with applicable law and the public interest.

(b) Information gathered and records retained by STTAS Components ***will not*** be:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. Disclosed or published without prior notice to the contributing agency that such information is subject to redisclosure or publication; or
3. Disseminated to unauthorized persons.

(c) Information will be disclosed to a member of the public who requests such information unless the disclosure of such information is exempt from disclosure by the California Public Records Act or applicable provisions of federal laws, regulations, and executive orders, which govern the disclosure of classified or sensitive but unclassified information.

(d) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

(e) An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

(f) There are several categories of records that will ordinarily ***not be provided*** to the public:

1. Public records required to be kept confidential by law are exempted from disclosure requirements under the Freedom of Information Act (FOIA), California Public Records Act (CPRA), Critical Infrastructure Information Act of 2002, among other provisions of law.
2. For instance, law enforcement records described in Gov Code §6254(f) will not be released to the public in accordance with the provisions of the CPRA.

(g) SAR information posted to the shared space or submitted to an external SAR repository may be disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the STTAS or STTAS Component mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the STTAS Component for this type of information.

(h) A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under various sections of the CPRA, including but not limited to sections 6254(f), (aa), (ab) and 6255. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

Disclosing Information to the Individual about Whom Information Has Been Gathered

(a) To the extent information is maintained in information systems controlled by the State of California, STTAS Components will comply with the Information Practices Act of 1977 and other applicable laws and regulations governing the disclosure of information to the individual about whom information has been gathered. To the extent consistent with these laws and regulations, the existence, content, and source of the information will not be made available to an individual when:

1. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
2. Disclosure would endanger the health or safety of an individual, organization, or community.
3. The STTAS Component did not originate, or does not otherwise have a right to disclose, the information.

Complaints and Corrections

(a) If an individual has complaints or objections to the accuracy or completeness of information retained about him or her *within a system under the Component's control*, the Component will advise the individual of the process to submit a request for correction by mail or e-mail. The request will document the individual's understanding of the record, the basis for his/her belief that the record is inaccurate, and the nature of the relief requested. The request should include all appropriate documentation. A record will be kept of all complaints and requests for corrections, the responsive action taken, if any, and a brief explanation of the rationale. An initial response to a complaint or request for correction must be made within 10 working days of receipt of the complaint or request. Unless the requested relief is granted, a final response must provide a brief discussion of the basis for a decision to deny the requested relief as well as information about the process of obtaining further review, reconsideration or appeal from the initial determination. This process will be specific to each STTAS Component. The appellate authority must be at an organizational level above the individual who made the initial decision. The STTAS Component Commander or his or her designee will determine whether the complaint or request involves ISE or FBI information and will review and approve the response.

(b) If an individual has complaints or objections to the accuracy or completeness of information about him or her that *originates with another agency*, the Component will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must either consent to the correction, remove the record, or assert a basis for denial in accordance with the California Public Records Act (CPRA) or Information Practices Act (IPA). This must be done in sufficient time to permit compliance with deadlines found within CPRA and/or IPA. A record will be kept of all complaints and correction requests. The existence, content, and source of the information will not be made available when, consistent with the CPRA and/or IPA, disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution; disclosure would endanger the health or safety of an individual, organization, or community; or the information is in a criminal intelligence system.

Review of Information Regarding Retention

(a) Information other than analytical product will be reviewed for purging every five years. Information may be reviewed through automated or other means consistent with resource constraints and availability. Records need not be individually examined to comply with this requirement. The date and means of review will be documented.

(b) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.

Security Safeguards

(a) The Assistant Director for Information Analysis, Watch and Warning is designated and trained to serve as the STTAS security officer.

(b) STTAS Components will operate in a secure facility protecting the facility from external intrusion. Each component will utilize secure internal and external safeguards against network intrusions. Access to databases from outside the facility will only be allowed over secure networks.

(c) STTAS Components will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

(d) Access to center information will only be granted to center personnel whose position and job duties require such access and the individual has successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

(e) Queries made to the component data applications will be logged into the data system identifying the user initiating the query.

(f) STTAS Components will maintain appropriate documentation to preserve audit trails of requested and disseminated information.

(g) Information will be marked appropriately if subject to specific handling caveats or other restrictions on storage, dissemination, use or destruction.

(h) To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

(i) Violations of this policy or internal operating policies at each STTAS Component will be reported to the STTAS Component Commander or his or her designee.

Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

2. When information has no further value or meets the criteria for removal according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

3. STTAS Components will delete information or return it to the source, unless it is validated, every five (5) years, in accordance with 28 CFR Part 23.

4. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period, as per item (2) above.

5. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.

6. A record of information to be reviewed for retention will be maintained by the component, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

SAR Information Retention and Destruction

1. All SAR information will be reviewed for retention annually. At the end of one year, SAR information must be either purged or converted into criminal intelligence files, if the information satisfies the requirements for submission into criminal intelligence files. SAR information may be retained if, at a minimum, all personally identifiable information (or privacy field information) is removed and purged.

Accountability and Enforcement

Information System Transparency

(a) The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through any public web sites providing information about the system.

(b) Each component will designate an individual who is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. Cal EMA will post contact information on its website. In most instances, this should be the same individual designated as the Privacy Officer.

Accountability for Activities

(a) Primary responsibility for the operation of the STTAC information systems—including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy—will be assigned in writing to a specific individual. Each Component will make its own determination about the specific individual or position within its center that is most appropriate to fulfill this responsibility.

(b) STTAS Components will protect information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions.

(c) STTAS Components will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

(d) STTAS Components will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law.

(e) STTAS Components will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy. Each center will provide a printed copy of this policy to all agency and nonagency personnel who provide services and will require of both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

(f) STTAS Components will periodically conduct audits and inspections of the information contained in its information systems. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

(g) STTAS Components will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

Inadvertent Disclosure

(a) The STTAC shall disclose any breach of the security of a State of California system involving personal data following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to

determine the scope of the breach and restore the reasonable integrity of the data system.

(b) With regard to computerized data that includes personal information that the STTAC does not own, component personnel shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if the STTAC or other law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number.
2. Driver's license number or California Identification Card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
4. Medical information.
5. Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. (3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

1. Written notice.
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
3. Substitute notice, if the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the STTAC does not have sufficient contact information. Substitute notice shall consist of all of the following:

    (A) E-mail notice when the agency has an e-mail address for the subject persons.
    (B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
    (C) Notification to major statewide media.

Enforcement

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the STTAS Component will take appropriate action based on the facts and circumstances of the specific incident. These include the following:

(a) Suspend or discontinue access to information by the user;
(b) Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;
(c) Apply other sanctions or administrative actions as provided in agency personnel policies;
(d) Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or
(e) Refer the matter to appropriate authorities for criminal prosecution, as necessary and appropriate, to effectuate the purposes of the policy.

Training

(a) STTAS Components will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

1. Component employees, contractors, and consultants;
2. Personnel providing information technology services to the agency;

3. Staff in other public agencies or private contractors providing services to the agency; and
4. Users who are not employed by the agency or a contractor.

(b) The training program will cover:

1. Purposes of the privacy, civil rights, and civil liberties protection policy;
2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;
3. The impact of improper activities associated with information accessible within or through the agency; and
4. The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

(c) STTAS Components will provide training to personnel authorized to share protected information in the ISE or e-Guardian. All reasonable efforts will be made to coordinate training efforts among the STTAS Components, where appropriate, to maximize the opportunity for training.

GOVERNANCE AND OVERSIGHT

The California State Terrorism Threat Assessment System (STTAS) Strategic Business Plan Concept of Operations (STTAS CONOPS) provides an overview of the five fusion center that comprise the STTAS. The governance structure and oversight mechanisms applicable to each STTAS Component are distinct and specific to a particular center.

Each STTAS Component will designate a trained privacy official who is responsible for handling reported errors and violations and, in accordance with specific direction and authorization, will be the focal point for ensuring that the center adheres to this policy and the provisions of the Information Sharing Environment Privacy Guidelines. The Commanders of the STTAS Components were responsible for the development of this policy. The drafting process was collaborative and included the staffs at each STTAS Component, as well as other state and local agencies and technical consultants at the national level. STTAS Component Commanders retain responsibility for ensuring that it is rigorously implemented and reviewed and updated annually.

As set forth above, each Commander, or his or her designee, is responsible for establishing and implementing appropriate procedures for resolving complaints involving SAR information or other matters associated with the handling of information. Each Commander, or his or her designee, will be responsible for information systems operations, as well as the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of

SAR information. STTAS Components will collaborate to ensure that best practices and training opportunities are made available to each Component to incorporate into its specific program as appropriate.

Definitions

Glossary of Terms and Definitions

Access
In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her. Access is an element of the Organization for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs). See *Fair Information Principles (FIPs).*

Access Control
The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Accountability Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Cooperation and Development (OECD). According to this principle, a data controller should be accountable for complying with measures that give effect to the principles stated above.

Audit Trail
Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Confidentiality
Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for, and to protect and preserve the privacy of, others. See *Privacy.*

Data Quality Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Cooperation and Development (OECD). According to this principle, personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date.

Data Transfer
As a key principle of privacy, it is the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

Disclosure
The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it.

Electronically Maintained
Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted
Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail. See *Extranet*.

Enforcement
A privacy principle that provides mechanisms for ensuring compliance with the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs), recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties.

Fair Information Principles (FIPs)
The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:
1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle

5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Homeland Security Information
As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Individual Participation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). As stated in the FIPs, according to this principle, an individual should have the right:

a) To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) To have communicated to him, data relating to him:
- Within a reasonable time;
- At a charge, if any, that is not excessive;
- In a reasonable manner; and
- In a form that is readily intelligible to him;

c) To be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and

d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Information
The use of data to extract meaning. Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips and leads data, and criminal intelligence data.

Information Disclosure
The exposure of information to individuals who normally would not have access to it.

Information Privacy
Information privacy is the interest individuals have in controlling or at least significantly influencing the handling of data about themselves.

Information Quality
The accuracy and validity of the actual values of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

Invasion of Privacy
Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also *Right to Privacy*.

Logs
Logs are a necessary part of an adequate security system, as they are needed to ensure that data is properly tracked and only authorized individuals are getting access to the data.

Metadata
In its simplest form, metadata is information (data) about information, more specifically information about a particular content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

Openness Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

Personal data
Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also *Personally Identifiable Information*.

Personal Information
See *Personally Identifiable Information*.

Personally Identifiable Information
Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to specify a unique individual.
The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Privacy
The term "privacy" refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy
A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and –implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Protected Information
Protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For local, state, and tribal governments, it would include applicable state and tribal constitutions and local, state, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public
Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Public Access
Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Purpose Specification Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, the purposes for which personal data are collected should be specified no later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Record
Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Retrievable Information
Information is retrievable in the ordinary course of business if it can be retrieved by taking steps that are taken on a regular basis in the conduct of business with respect to that information or that an organization is capable of taking with the procedures it uses on a regular basis in the conduct of its business. Information is not considered retrievable in the ordinary course of business if retrieval would impose an unreasonable burden or violate the legitimate rights of a person that is not the subject of the information. The unreasonableness of burden is balanced against the significance of the information's use.

Secondary Data Uses
Uses of personally identifiable information for purposes other than those for which the information was originally collected. The Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs) state that a person can provide personally identifiable information for a specific purpose without the fear that it may later be used for an unrelated purpose without that person's knowledge or consent.

Security Policy
A security policy is different from a privacy policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. A security policy addresses information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy. See *Privacy Policy*.

Security Safeguards Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Transborder Flows of Personal Data
Movements of personal data across national borders. See *Fair Information Principles (FIPs)*.

Use
With respect to personally identifiable information, the sharing, employment, application, utilization, examination, or analysis of such information within the agency or organization that maintains the designated record set.

Use Limitation Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law. See *Purpose Specification Principle*.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. MIAMI-DADE POLICE DEPARTMENT'S FUSION CENTER PRIVACY POLICY

HOMELAND SECURITY BUREAU – MIAMI-DADE FUSION CENTER PRIVACY POLICY

The **Miami-Dade Police Department's Homeland Security Bureau** is a Fusion Center (herein referenced to as **"HSB"** or **"Center"**) as defined below:

The HSB was initiated in response to the increase need for timely information sharing and exchange of crime related information among members of the law enforcement community. One component of HSB focuses on the development and exchange of criminal intelligence. This component focuses on the criminal intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

The goal of establishing and maintaining the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center criminal intelligence system is to:

- Increase public safety and improve national security.
- Minimize the threat and risk of injury to citizens.
- Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety or health.
- Minimize the threat and risk of danger to real or personal property.
- Protect individual privacy, civil rights, civil liberties, and other protected interest.
- Protect the integrity of the criminal investigatory, criminal intelligence, and criminal justice system process and information.
- Minimize reluctance of individuals or groups to use or cooperate with the justice system.
- Promote governmental legitimacy and accountability.
- Make the most effective use of public resources allocated to public safety agencies.

MISSION STATEMENT:

The Mission of the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center is to enhance partnerships which foster a connection between every facet of the law enforcement community. HSB will afford the men and women, who are dedicated to protecting the public and addressing violence, with all available intelligence resources and communications capabilities. Unless readily shared, critical information is without value.

HSB's criminal intelligence products and services will be made available to law enforcement agencies and other criminal justice entities with a demonstrated right and need to know. All agencies who participate in HSB will be subject to a Memorandum of Understanding and will be required to adhere to all HSB's policies and security requirements. The purpose of this Privacy Policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

All Center personnel will comply with all laws protecting privacy, civil rights and civil liberties and adhere to the guidelines set forth in 28CFR Part 23. HSB will provide a printed copy of this policy to all department and non department personnel who provide services and will require of both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

GUIDING PRINCIPLES:

HSB's Privacy Policy has eight Privacy Design Principles which shall guide the policy and practices wherever applicable. The eight Privacy Design principles are:

1. **Purpose Specification** – Define the HSB's purpose for information to help ensure the agency uses of information is appropriate.
2. **Collection Limitation** – Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality** – Ensure data accuracy
4. **Use Limitation** – Ensure appropriate limits on Department use of personal information.
5. **Security safeguards** – Maintain effective security over personal information
6. **Openness** – Maintains a citizen access to information available through the Freedom of Information Act.
7. **Individual Participation** – Allow individual's reasonable access and opportunity to correct errors in their personnel information held by the Agency.
8. **Accountability** – Identify, train and hold agency personnel accountable for adhering to agency information quality and privacy policies.

I. Purpose Specification

HSB has developed databases by using existing data sources from federal, state and local law enforcement agencies. HSB will have the capability to combine data with the goal of identifying, developing and analyzing information related to violent crime or terrorist activity for investigative leads. This capability will facilitate integration and exchange of information between participating law enforcement agencies.

II. Collection Limitation

HSB is maintained for the purposes of developing information and criminal intelligence by agencies who participate in the Center. The decision of an agency to participate in Center and which databases provide information is voluntary. Information obtained and disseminated by a law enforcement agency outside of Miami-Dade will be governed by that agency's local, state and federal laws as well as their respective policies.

Because the laws, rules or policies governing information and criminal intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Therefore, each contributor of information is under different legal restraints and restrictions. Each agency has its own responsibility to abide by the collection limitations applicable to it by reasons of law. Information contributed to the center should be that which has been collected in conformance with those limitations and has been vetted for legal sufficiency.

III. Data Quality

The agencies participating in the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. Each contributor or contributing agency is solely responsible for data accuracy and quality.

The provisions set forth in this Privacy Policy will be reviewed annually during the first month of the year.

IV. Use Limitation

Information obtained from or through the HSB can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

The primary responsibility for the overall operation of the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center will rest with the Major of the Homeland Security Bureau of the Miami-Dade Police Department. The Major will enforce the Privacy Policy of the HSB and take the necessary measures to make certain that access to the HSB's information and resources is secure and will prevent any unauthorized access or use. The Miami-Dade Police Department reserves the right to restrict the qualifications and number of personnel who will be accessing HSB and to suspend or withhold service to any individual violating this Privacy Policy. The Department, or persons acting on behalf of the Department, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

Security for information derived from HSB will be provided in accordance with all applicable federal, state and local laws, the rules and regulations of the Miami-Dade Police Department, and HSB policies. Furthermore, all personnel who receive, handle, or have access to HSB data and/or sensitive information will be trained as to those requirements. All personnel having access to the HSB's data agree to abide the following rules:

1. HSB's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer and HSB.
2. Individual passwords will not be disclosed to any other person except as authorized by the Department.
3. Individual passwords will be changed if authorized personnel of the Department, the HSB or any individual password holder suspects the password has been improperly disclosed or otherwise compromised.
4. Background checks will be completed on personnel who will have direct access to HSB.
5. Use of HSB's data in an unauthorized or illegal manner will subject the user to denial of further use of the HSB; discipline by the user's employing agency, and /or criminal prosecution.

Each authorized user understands that access to the HSB can be denied or rescinded for failure to comply with the application restrictions and use limitations.

V. Security Safeguard

Information obtained from or through the HSB will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Use of HSB's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the HSB will be granted only to law enforcement agency personnel, sworn or non-sworn, who have been screened with a state and national fingerprint-based background check, as well as any additional background screening process using procedures and standards established by the *Miami-Dade Police Department*.

The Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center operates in a secure facility, protecting the HSB from external intrusion. The HSB will utilize secure internal and external safeguards against network intrusions. Access to HSB databases from outside the facility will only be allowed over secure networks.

HSB will store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such action.

The Intelligence Section Lieutenant will serve as a security officer in addition to their regular supervisory duties. The Lieutenant will be responsible for the physical, procedural, and technical safeguards of the HSB.

VI. Openness

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

HSB is a collection of various databases, which allows the Department and participating agencies to share information and to accelerate the dissemination of information already collected. HSB does not change or alter a citizen's rightful access to information accorded to them under state law. The HSB follows Florida State Statute 119 – Public Records Laws.

VII. **Individual Participation**

The data maintained by HSB is provided, on a voluntary basis, by the participating agencies or is information obtained by other sources. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretations, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the HSB's applications. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question. Participating agencies agree that they will refer request related to privacy or sunshine laws back to the originator of the information.

VIII. **Accountability**

When a query is made to any of the HSB's data applications, the original request is automatically logged by the HSB's Intelligence Analysis Supervisor or the Sergeant into the log system which will identify the user initiating the query. When such information is disseminated outside the agency from which the original request is made, a second dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for law enforcement investigative purpose or other agencies as provided by law. The agency from which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

1. Date of release.
2. To whom the information relates
3. To whom the information was released (including address and telephone number)
4. All identification numbers or other indicator that clearly identifies the data released.
5. The purpose for which the information was released.

The Miami-Dade Police Department will be responsible for conducting or coordinating audits and investigating misuse of data information. All violations and/or exceptions shall be reported to the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center. Individual users of the

HSB's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use of limitations for the use of HSB's data may result in the suspension or termination of used privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the Center is required to abide by this *Privacy Policy* in the use of information obtained by and through the Center.

Training

The Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center will always encourage training and provide and seek out specialized training programs for personnel assigned to the HSB. The intent of training is to develop a culture of information analysis and information sharing within the Miami-Dade Police Department's Homeland Security Bureau / Miami-Dade Fusion Center.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Andino, R. (2008). The privacy challenges of U.S. fusion centers. *Privacy Advisor*. Retrieved August 28, 2009, from http://highlighttech.com/pdf/FusionCenters_doc.pdf

California. (2009). California State Terrorism Threat Assessment System Information Privacy Policy.

Chicago Police Department. (2009). Crime Prevention and Information Center Privacy Policy.

Coney, L. (2007). Statement, Department of Homeland Security Data Privacy and Integrity Advisory Committee. Retrieved August 28, 2009, from http://epic.org/privacy/fusion/fusion-dhs.pdf

Electronic Privacy Information Center. (2009). Memorandum of understanding between FBI and Virginia State Police. Retrieved August 28, 2009, from http://epic.org/privacy/virginia_fusion/MOU.pdf

Geiger, H. (2009). Fusion centers get new privacy orders via DHS grants. Center for Democracy & Technology. Retrieved July 14, 2010, from http://www.cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants

General Accounting Office. (2008). Privacy: Congress should consider alternatives for strengthening protection of personally identifiable information. Statement of Linda D. Koontz, Director, Information Management Issues, testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.

German, M. & Stanley, J. (2007). What's wrong with fusion centers? Retrieved August 28, 2009, from http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf

German, M. & Stanley, J. (2008). Fusion center update. Retrieved August 28, 2009, from http://www.aclu.org/pdfs/privacy/fusioncenter_20081212.pdf

Gersten, D. (2009). The future of fusion centers. Testimony of Acting Deputy Officer for Programs and Compliance David D. Gersten, Office for Civil Rights and Civil Liberties, before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Retrieved August 28, 2009, from http://www.dhs.gov/ynews/testimony/testimony_1238617488915.shtm

Information Sharing Environment. (2008). Privacy and civil liberties implementation guide for the information sharing environment. Washington, DC: Office of the Director of National Intelligence.

Information Sharing Environment. (2010). Annual report to the Congress. Washington, D.C: Office of the Director of National Intelligence. Retrieved September 6, 2010, from http://www.ise.gov/document/ISE_AR-2010_Final_2010-07-29.pdf

Lane, F. (2009). American privacy. The 400-year history of our most contested right. Boston: Beacon Press.

Miami-Dade Police Department. Homeland Security Bureau Privacy Policy.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission Report*. New York: W.W. Norton & Company, Inc.

O'Harrow, Jr., Robert. (2008, April 2). Centers tap into personal databases. *Washington Post*. Retrieved August 28, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html

Privacy Office. (2007). Privacy Impact Assessments Official Guidance. Retrieved August 23, 2010, from http://www.dhs.gov/xlibrary/assets/privacy/privacy

Relyea, H. (2002). The Privacy Act: Emerging issues and related legislation. Washington, D.C.: Congressional Research Service, RL30824.

Riegle, R. (2009). The future of fusion centers: Potential promise and dangers. Testimony of Director Robert Riegle, State and Local Program Office, Office of Intelligence and Analysis, before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. Retrieved August 28, 2009, from http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm

Rollins, J. (2008). Fusion centers: Issues and options for Congress. Washington, D.C.: Congressional Research Service, RL34070.

Rollins, J. & Connors, T. (2007). State fusion center processes and procedures: Best practices and recommendations. Retrieved August 2, 2010, from http://www.manhattan-institute.org/pdf/ptr_02.pdf

Suspicious Activity Report Support and Implementation Project. (2008). Findings and recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project. Retrieved September 6, 2010, from https://www.hsdl.org/?view&doc=108116&coll=limited

United States Department of Homeland Security. (2008). Privacy impact assessment for the Department of Homeland Security state, local, and regional fusion center initiative. Washington, DC.

United States Department of Homeland Security & Department of Justice. (2006). Fusion center guidelines: Developing and sharing information and intelligence in a new era. Washington, DC.

United States Department of Justice. (2008). Privacy and civil liberties policy development guide and implementation template. Washington, DC.

United States Department of Justice. (2009). U.S. Department of Justice's global justice information sharing initiative. Washington, DC.

Federal Statutes

E-Government Act of 2002, 44 U.S.C. § 208.

Privacy Act of 1974, 5 U.S.C. § 552a.

Title 28 Code of Federal Regulations, Part 23.

Case Law

City of Ontario v. Quon, 560 U.S. ___ (2010). Retrieved September 3, 2010, from http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf

Griswold v. Connecticut, 381 U.S. 479 (1965).

Katz v. U.S., 389 U.S. 347 (1967).

Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).

Smith v. Maryland, 442 U.S. 735 (1979).

Terry v. Ohio, 392 U.S. 1 (1968).

United States Constitution.

U.S. v. Miller, 425 U.S. 435 (1976).

U.S. v. U.S. District Court, 407 U.S. 297 (1972).

U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

Whelan v. Roe, 429 U.S. 589 (1977).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California